NAStorage 4600 / 12600 / 12620 Series

Tower / 1U / 2U Rack mount

User Manual

Rev. 1.1

Electronic Emission Notice

Federal Communications Commission (FCC)
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Notice

This device complies with the EMC directive of the European Community and meets or exceeds the following technical standard: EN 55022 ~ “Limits and Methods of Measurement of Radio interference Characteristics of information Technology Equipment.” This device complies with CISPR Class A standard. (The 4600T complies with Class B standard.)

Warning:
This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

CE

Safety Information

To reduce the risk of fire or electric shock, install the unit in a temperature-controlled indoor area free of conductive contaminants. Do not place the unit near liquids or in an excessively humid environment.
Do not allow liquids or foreign objects to enter the unit. All servicing of this equipment must be performed by qualified service personnel. Remove rings, watches and other jewelry before servicing the unit.
Before maintenance, repair or shipment, the unit must be completely switched off and unplugged and all connections must be removed.

Safety Notices:

The computer may provided with CD drives comply with appropriate safety standards including IEC 60825

Caution:
This unit is provided real-time clock circuit. There is
a danger of explosion if battery is incorrectly replaced. Replace only with 3-Volt Lithium cell (CR2032) or equivalent type. Discard used batteries according to the manufacturer's instructions.

Caution:
Before connect or disconnect power cord of the power supply, ensure to turn the power supply switch OFF to avoid the risk of equipment damage.

Revision History

Rev. 1.0: Initial release.

Rev. 1.1: Added functional description for the 12620U model and changes in the firmware features.

Table of Contents

Electronic Emission Notice• 2
Safety Information• 3
Table of Contents• 4

Chapter 1 Introduction• 7

1.1 Features• 7
1.2 Conventions• 7
1.3 Overview• 8

4600T Front View• 8
4600U Front View• 10
4600U Rear View• 10
12600 Series Front View• 11
12600U Rear View• 11
12620U Rear View• 11
System LED Definitions • 12

Chapter 2 Installing and Starting the NAS System• 13

2.1 Hardware Installation - 4600T• 14
2.2 Interface Connections - 4600T• 17
2.3 Hardware Installation - Rackmount Enclosures (4600U, 12600U, 12620U)• 18
2.4 Hardware Installation - Rackmount Enclosures (12600U & 12620U)• 23
2.4 Installing Disk Drives - 4600U, 12600U and 12620U• 26
2.5 Optional PCI-E adaptor installation (Only for 12600U & 12620U)• 27
2.6 Connecting Expansion Enclosures (for 12600U & 12620U) • 28
2.7 Starting the System • 30
2.8 Shutting Down the System • 30
2.9 Drive Tray LED Definitions • 31
2.10 Install the NASFinder Utility • 32
2.11 Using the Top Screen Tools • 36
2.12 Configuring IP Address Using the LCD Keypad (Tower 4600T Only) • 37

Chapter 3 Managing & Setup: System• 40

3.1. System General Page• 40
3.2. System > Overview• 42
3.3. System > General• 43
3.4. System > Network • 43

3.4.1 System > Network > Information• 43
3.4.2 System > Network > LAN/IP• 44
3.4.3 SSL Settings • 47

3.5. System > Maintenance• 55
3.6. System > Configuration• 67
3.7. System > System Log• 69

3.7.1 System > System Log > Syslog Remote• 70

3.8. System > Platform IPMI• 71

Chapter 4 Storage• 72

4.1. Storage > Disks • 72
4.2. Storage > Volumes • 78
4.2.1 Volumes• 79
4.2.2 Disk Operation• 83
4.2.3 External FAT/NTFS• 87

4.3 Storage > Folder Groups• 88
4.3.1 Folder Groups• 88
4.3.2 Storage > Folder Groups > Files & Folders• 90
4.3.3 Storage > Folder Groups > Folder Group Options• 91
4.3.4 Storage > Folder Groups > User Quota• 94

4.4. Storage > Logical Disks • 95
4.5. Storage > Snapshots • 97

Chapter 5 Account• 98

5.1. Account > System • 98
5.2. Account > Windows AD • 100
5.3. Account > UNIX NIS • 104
5.4. Account > Permission • 105
5.5. Account > Permission > ACLs• 107
5.6. Account > Permission > Effective• 109

Chapter 6 Service• 111

6.1. Service > Status • 111
6.2. Service > Windows • 112
6.3. Service > Apple• 113
6.4. Service > Unix NFS• 114
6.5. Service > FTP• 115
6.6. Service > iSCSI Targets • 117
6.7. Service > Rsync • 127
6.7. Service > Replication • 128

Chapter 7 Share• 131

7.1. Share - Adding Shares • 131
7.2. Share - Edit or Delete• 132

Chapter 8 Backup• 134

8.1. Backup - Rsync • 134
8.2. Backup - Local Copy • 136
8.3. Backup - Replication • 137

Chapter 9 Antivirus• 142

9.1. Antivirus > Information • 142
9.2. Antivirus > Antivirus Tasks• 143
9.3. Antivirus > Virus Scan Record• 145

Chapter 10 Event• 146

10.1. Event > Configuration •..... 146
10.2. Event > Reminder • 147
10.3. Event > System • 148
10.4. Event > Device • 149
10.5. Event > Security• 150

Chapter 11 Status•..... 152

11.1. Hardware • 152
11.2. Status > Opened Files•..... 153
11.3. Status > Connections• 153
11.4. Status > Task Progress• 154
11.5. Status > Loading• 155

Appendix A More about RAID Storage• 156

The Key Differences between the 4600U/T and the 12600 Models.

- The 4600U/T series does not support the Dedup, Copy, and Sync disable functions. The Compression function is supported.
- The 12600U series supports Dedup, Compression, and yet the Copy and Sync functions can not be disabled.

Chapter 1 Introduction

1.1 Features

The NAS server is a premier NAS product featuring tera-bytes of massive storage capacity and full-range data protection to provide a cost-effective, highly reliable and high-performance storage system for the fast growing network storage demand.

- Deliver storage capacity over tera-bytes
- Expand RAID storage capacity without downtime
- Feature with hot-swappable HDD to maximize storage flexibility
- Accelerate network throughput with the dual-NIC and Gigabit Ethernet support
- Seamless integration into heterogeneous networking security
- Backup and archive important data to USB, eSATA devices, a local or remote storage server.

1.2 Conventions

Terminology
The term “NAS server” means all the models of the network attached storage servers unless the specific model is mentioned.
Typographic Conventions
Conventions: Meaning
Italic: Variable name, which should be replaced by user-defined text in context
Bold: Menu item or functions
Underline: Cross-reference

Symbols and Statements in this Document

NOTE: Notices provide guidance or advices that are related to the functional integrity of the machine.

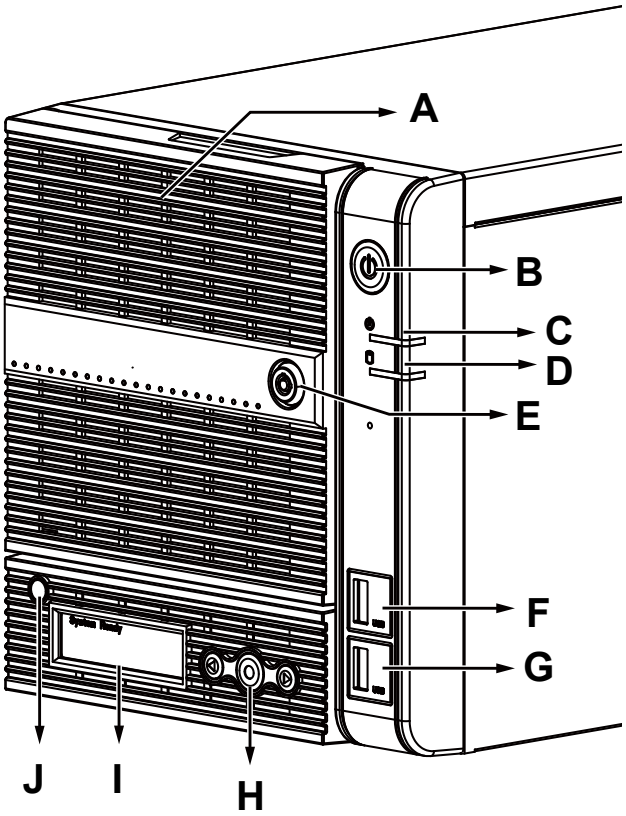
Tips: Tips are useful information that helps enhance or facilitate an installation, function, or process.

WARNING! or **IMPORTANT**: These statements indicate situations that can be dangerous or hazardous to the machine or you.

Electrical Hazard: This statement appears when high voltage electrical hazards might occur to an operator.

1.3 Overview

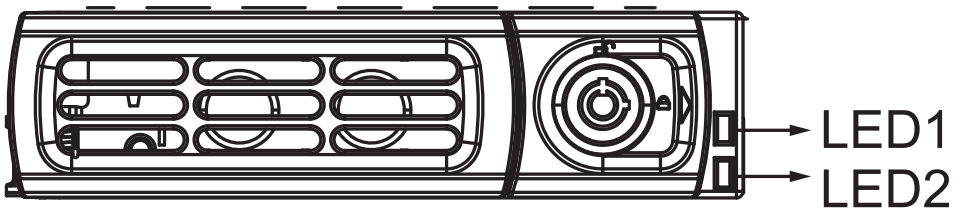
4600T Front View



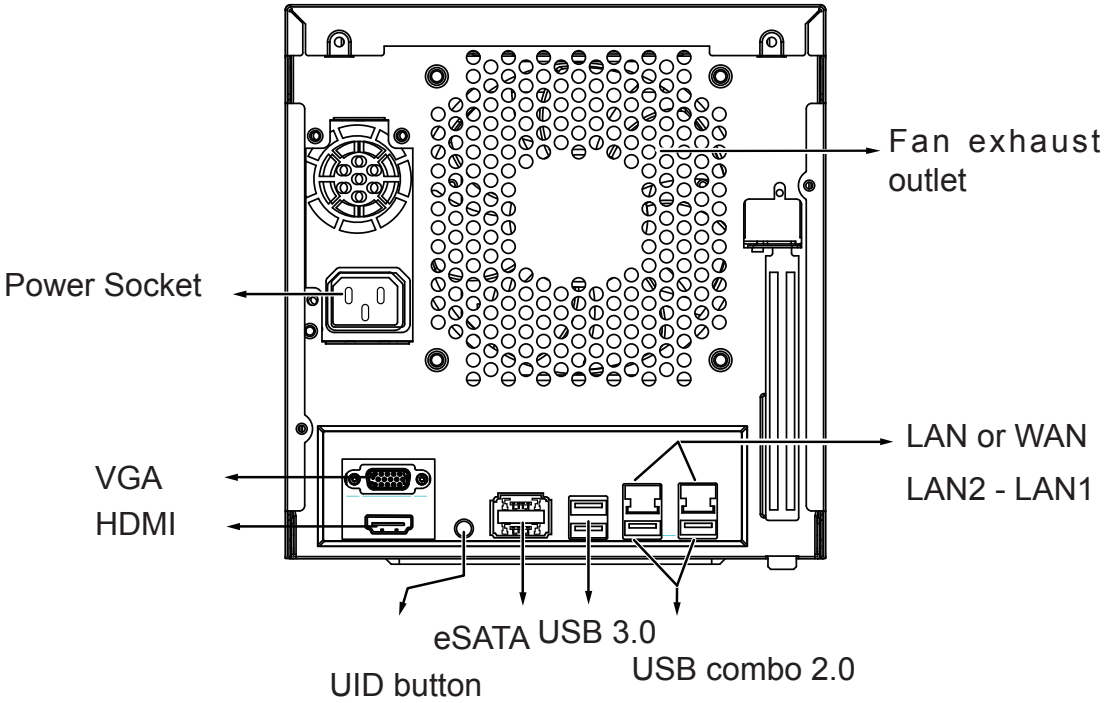
A	Front cover, it can protect your hard disks cannot be easily removed by unauthorized persons.
B	Power button. NOTE: This power button is only enabled when NAS front cover is opened, it's a secure design to defend invader from powering off the system.
C	Power LED - blue
D	System Read/Write LED - Orange
E	Front cover bezel lock.
F	USB port (For backup data).
G	USB port (For backup data).
H	LCM control buttons (Left/Enter/Right).
I	LCM for system status display and IP address settings
J	System status LED. System Normal: Green System Warning or Faults occurred: Red

4600T LED Definitions

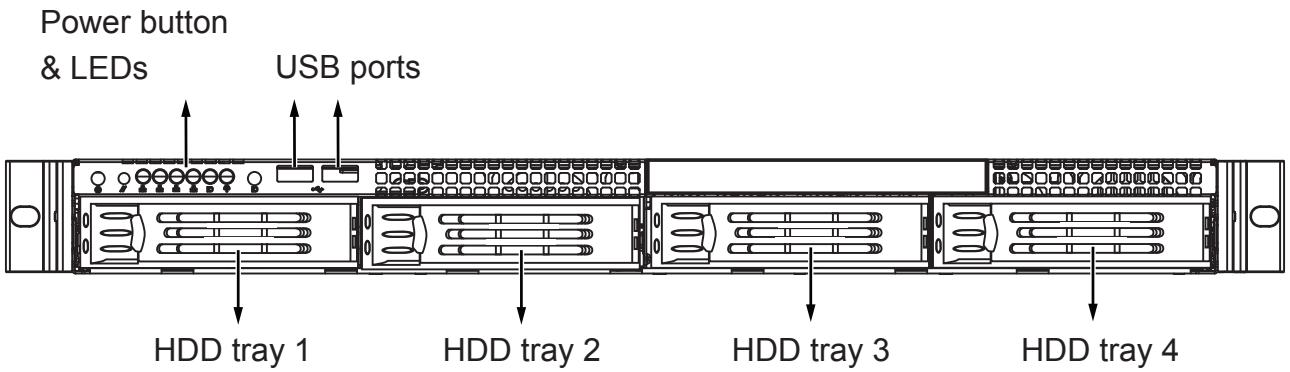
LED1 (Status / error)	LED2 (Disk access)	Definition
Constant Green	OFF	No access to H.D.D.
Constant Green	Blinking Green	Access to H.D.D.



4600T Rear View



4600U Front View

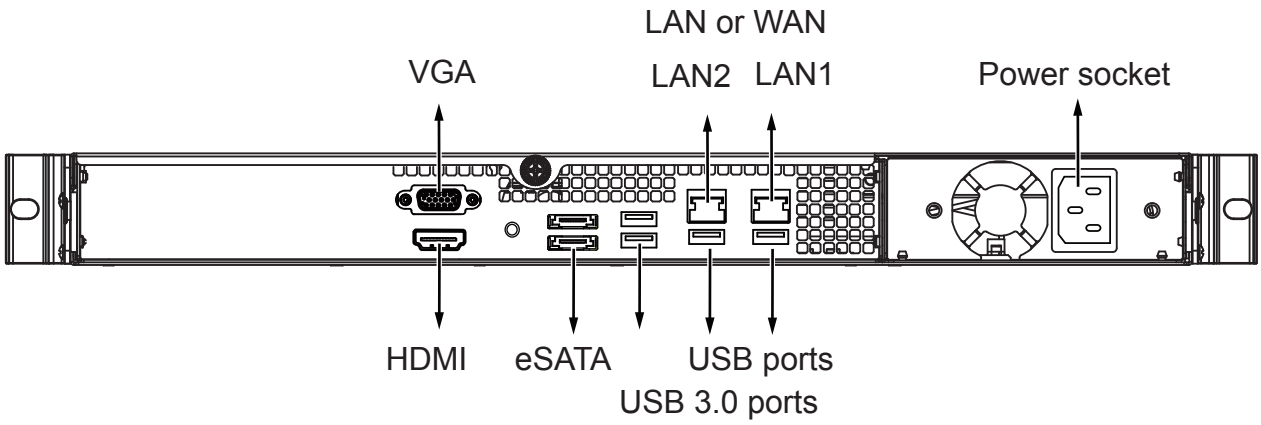


4600U LED & Push button Definitions

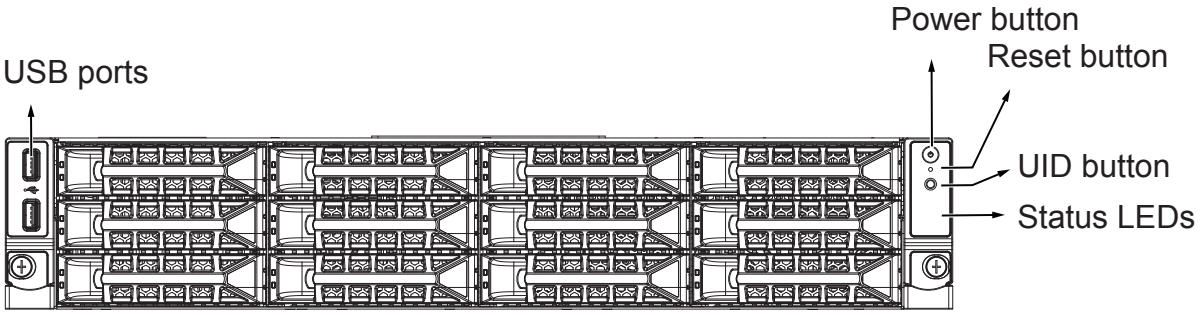
* Items are listed according to their positions from left to right.

LED / Button	Definition
Power button	Power the system on or off (pressed for one second)
Reset button	Resets the system
LAN1 LED	Network transaction status
LAN2 LED	Network transaction status
UID LED	Indicates the system is currently being identified. Pressing the Server Identify button will also light up the LED.
System Status LED	Displays the system operating statuses
UID button	Lights the UID LED & system notification

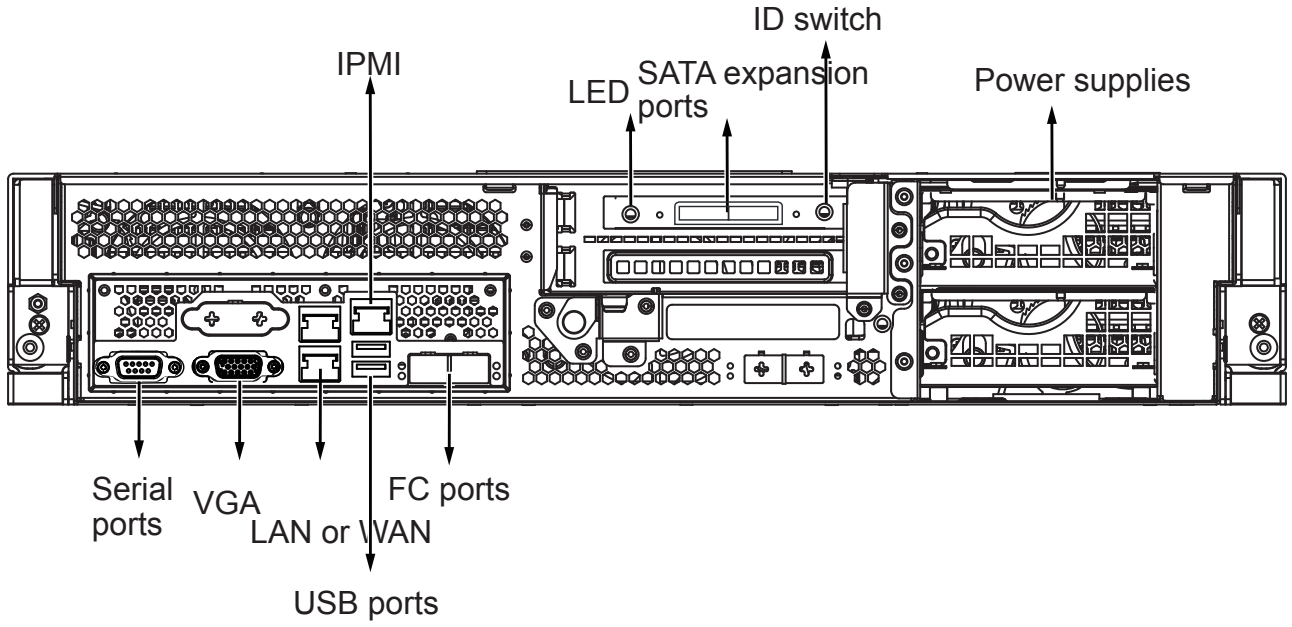
4600U Rear View



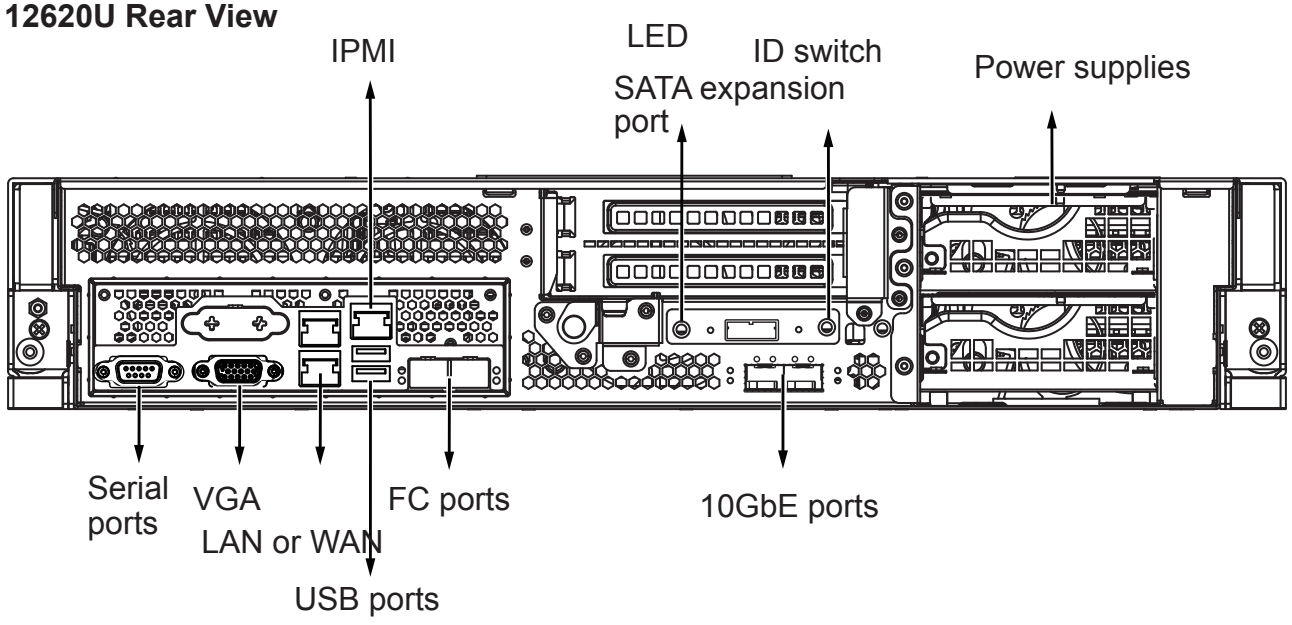
12600 Series Front View



12600U Rear View



12620U Rear View



System LED Definitions

Front Panel		
Indicator/error	**Color**	**Description**
System Status (BMC) - ON	Amber	Event in BMC marked with *** has happened
System Status - Blinking	Amber	Voltage sensor critical
System Status - ON	Green	System working normally
System Status - Blinking	Green	Fan/Temp sensor critical or chassis intrusion alert
HDD - Blinking	Green	Internal SATA DOM activities
BMC	-	No function
UID - Blinking	**Blue**	**The chassis is being indicated**
UID - OFF	**Blue**	**The chassis is not being indicated**
LAN1 (GbE) - ON	**Green**	**Linked**
LAN1 - Blinking	**Green**	**LAN activities (off when there is no traffic)**
LAN1 - OFF	**Green**	**Disconnected**
LAN2 (GbE) - ON	**Green**	**Linked**
LAN2 - Blinking	**Green**	**LAN activities (off when there is no traffic)**
LAN2 - OFF	**Green**	**Disconnected**

Front Panel		
Indicator/error	**Color**	**Description**
LAN3 (10GbE) - ON	**Green**	**Linked**
LAN3 - Blinking	**Green**	**LAN activities (off when there is no traffic)**
LAN3 - OFF	**Green**	**Disconnected**
LAN4 (10GbE) - ON	**Green**	**Linked**
LAN4 - Blinking	**Green**	**LAN activities (off when there is no traffic)**
LAN4 - OFF	**Green**	**Disconnected**

Drive Tray LED		
Indicator/error	**Color**	**Description**
OFF	**Red**	**No fault, and is not being indicated**
Blinking - 4Hz	**Red**	**The drive is being indicated**
Blinking - 1Hz	**Red**	**RAID rebuild is taking place**
ON	**Red**	**Drive faults have occurred**

Chapter 2 Installing and Starting the NAS System

This chapter covers the installation procedure of different form factors of NAS server in the tower or rack-mount chassis. Instructions on how to startup the NAS server by setting up the basic configuration through the Admin Home page or provided software tool – NASFinder is also outlined in this chapter.

2.1 Installing the NAStorage controller&mobile rack

Package Contents

NAS server controller package:

- Two RJ-45 ports and one serial connector
- Two Ethernet cables
- NAS server Quick Installation guide
- NAS server utilities CD

4600U rack-mount model package:

- One slide rail package for fitting into an 19" rack cabinet.

⚠ IMPORTANT:

1. It is important to leave a clearance of 15cm to the rear side of the chassis. The clearance is required to ensure an adequate airflow through the chassis to ventilate heat. A 5cm clearance is also required on both sides of the chassis.

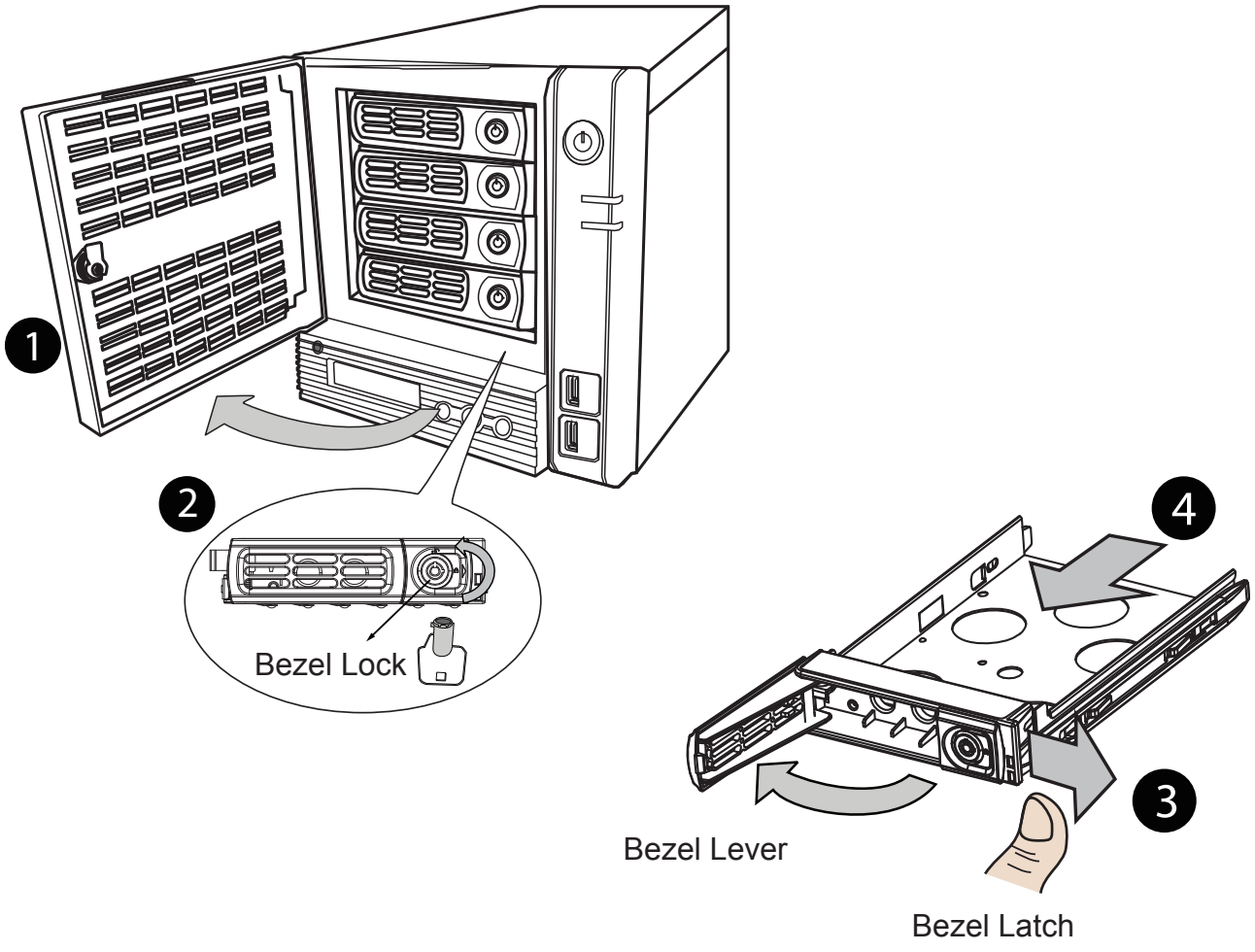
   To ensure normal operation, maintain ambient airflow. Do not block the airflow around chassis such as placing the system in a closed cabinet.

2. For a RAID volume configuration, it is recommended you use hard drives of the same model featuring the same capacity and rotation speed, even running the same version of firmware.

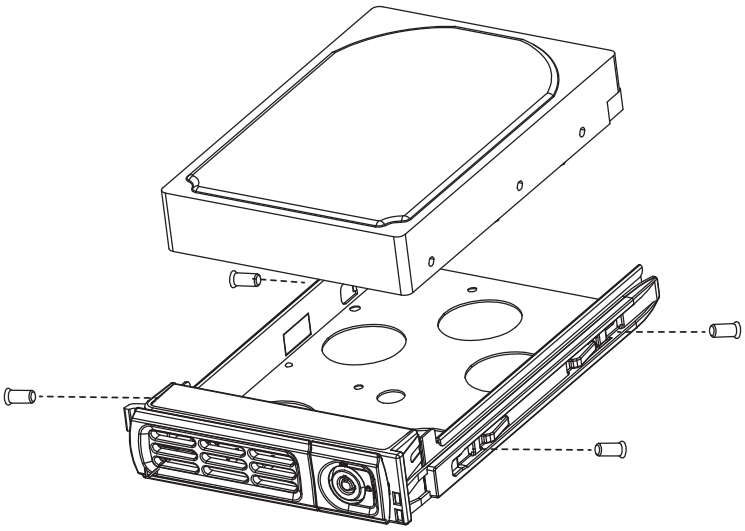
2.1 Hardware Installation - 4600T

SATA hard disk(s) are user-supplied. The NAS server can readily accommodate most of the off-the-shelf SATA hard drives. For the latest compatibility list, please check on our website.

1. Use the included bezel key to open the front panel.
2. Use the included bezel key to unlock the bezel lock on drive trays.
3. Open the drive tray bezel by flipping the bezel latch to the side. The bezel lever will spring open.
4. You can then remove the drive tray.



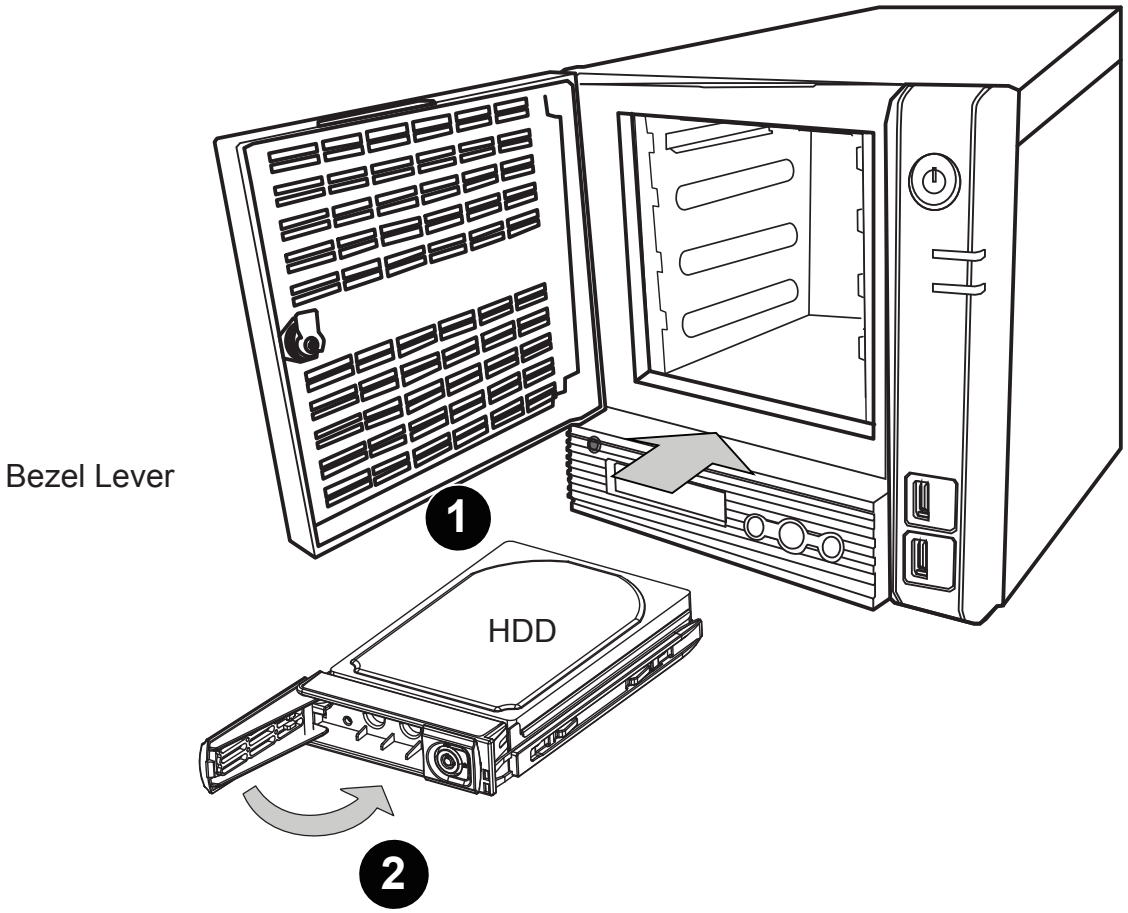
4. Install your hard disk to the drive tray. Gently put the hard disk into drive tray with its label side facing up and the connector side facing the inside of the chassis. Secure the hard drive by fastening 4 screws from both sides.



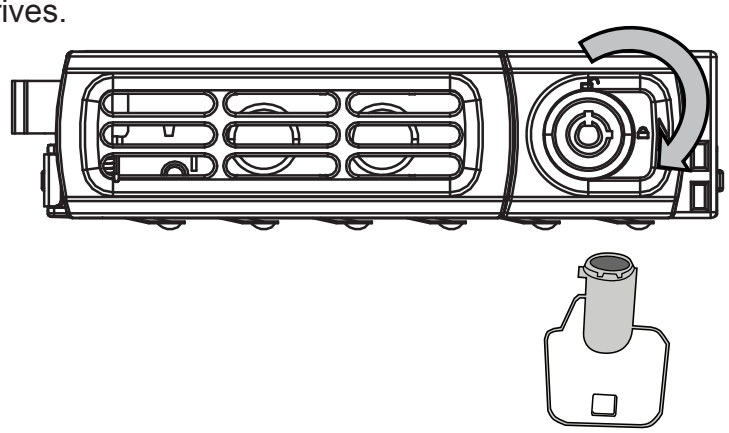
IMPORTANT:

Avoid touching the hard drive's circuit board or connector pins. Doing so can damage the hard drive by electro-static discharge.

5. Install drive tray by pushing it into drive bay. when it is almost fully inserted, close the bezel. The bezel will secure the back-end connection to the backplane.

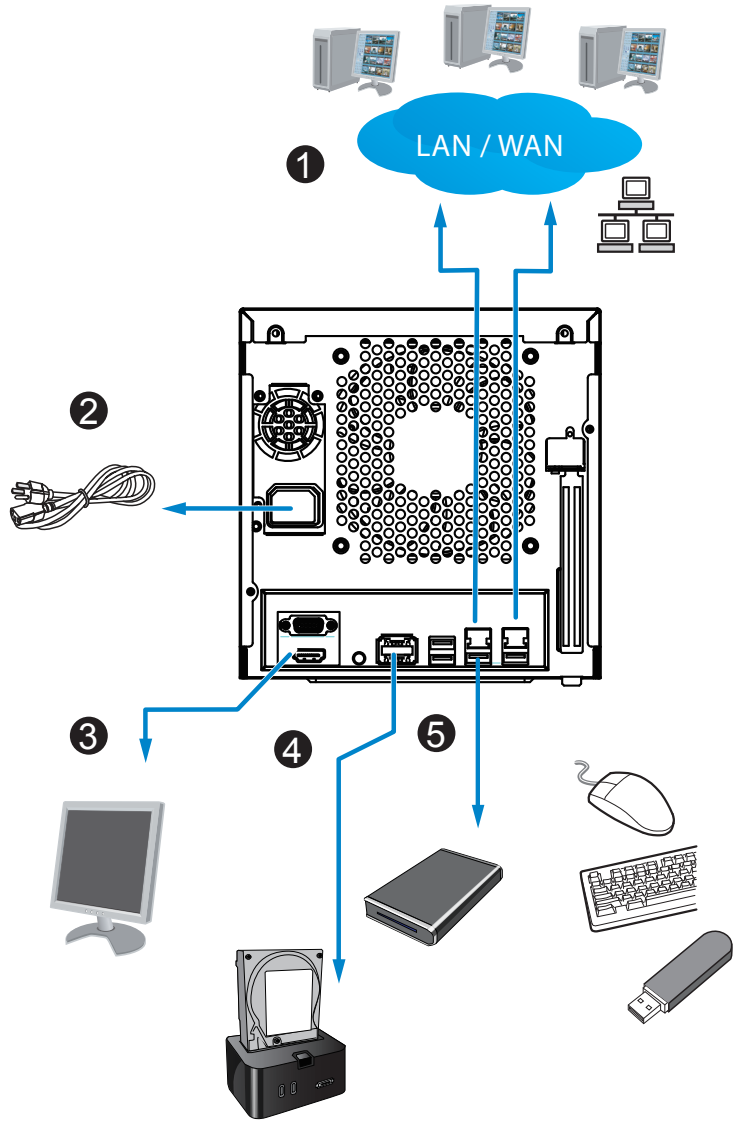


6. Use the bezel key to lock the drive tray. Repeat the above process to install more disk drives.



Bezel Lock

2.2 Interface Connections - 4600T



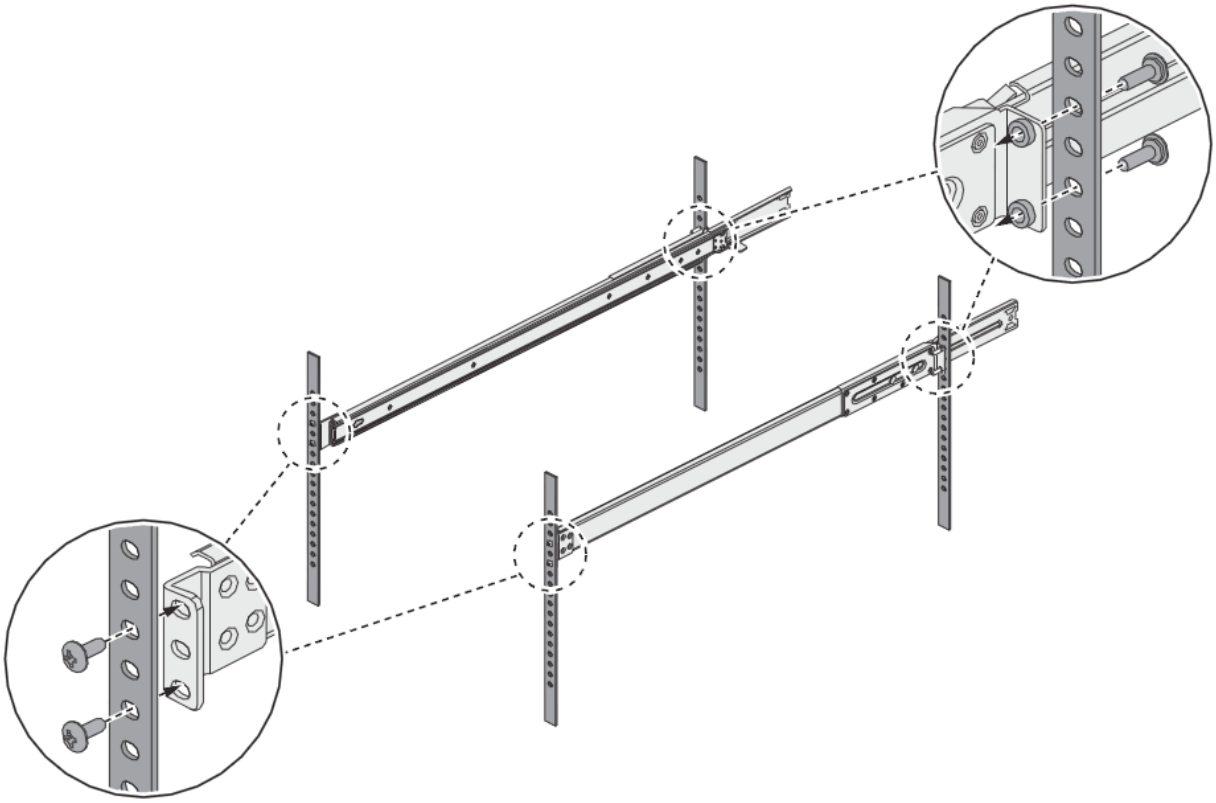
Item no.	Description
1	Connect LAN ports to a local area network
2	Power cord to the power supply (110~240V, 3.5A, 47~63Hz).
3	15-pin VGA and HDMI to monitor.
4	eSATA port for backup to external storage devices.
5	USB ports to USB devices, e.g., thumb disks for backup, keyboard, and mouse.

2.3 Hardware Installation - Rackmount Enclosures (4600U, 12600U, 12620U)

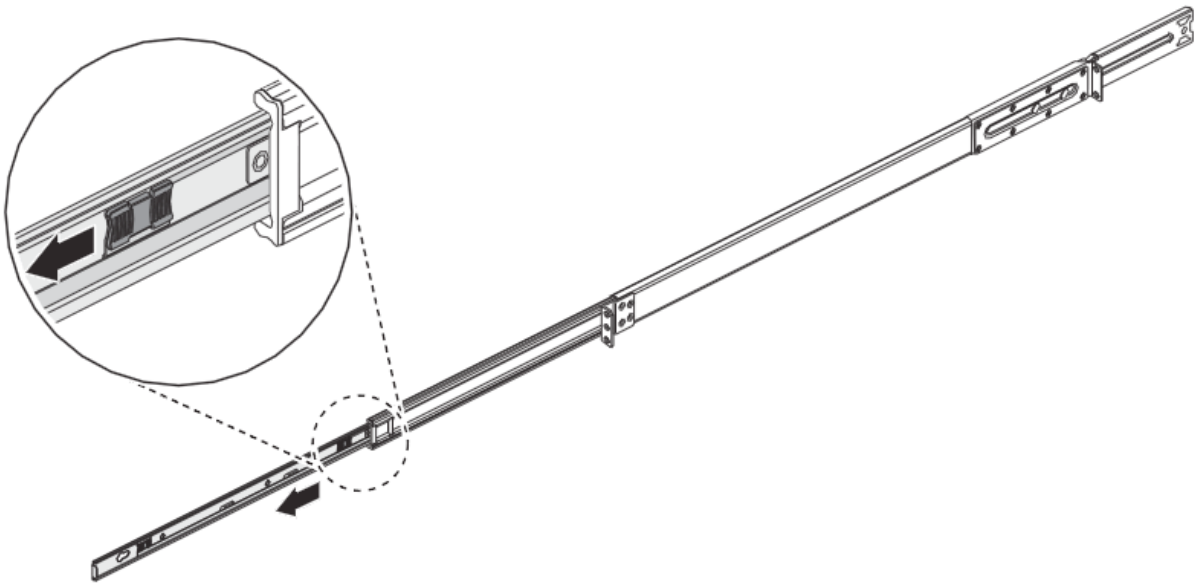
The mounting holes and installation methods are identical for the rack-mount models 12600U and the 12620U.

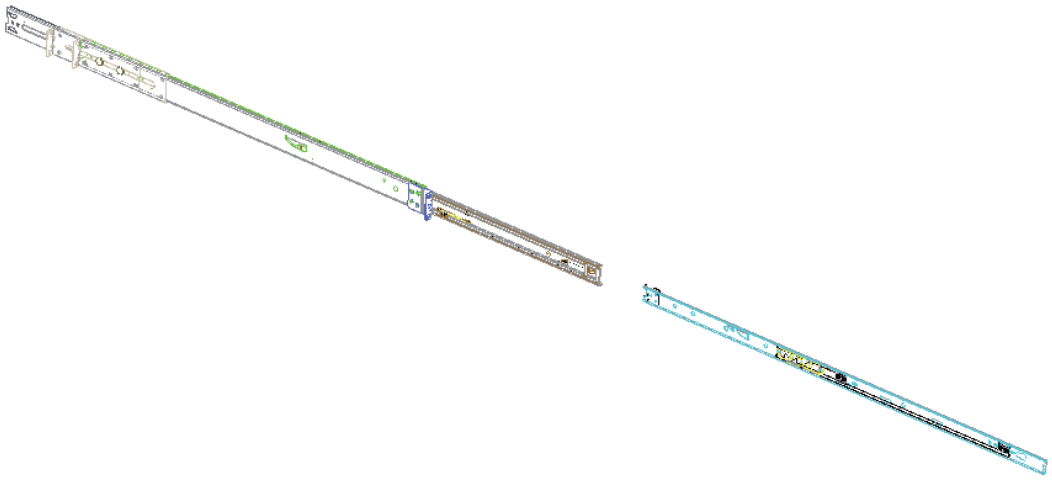
Follow the procedure to install a rackmount enclosure to a rack cabinet:

1. Remove all HDD trays from the server.
2. Secure the left- and right-side slide rails to the rack posts.
   Secure the rails to rack posts using 8 of the included pan head screws.
   Use screws (P/N:2A5816C00-600-G) for square-hole racks.
   Use screws (P/N:2A5816D00-600-G) for round-hole racks.

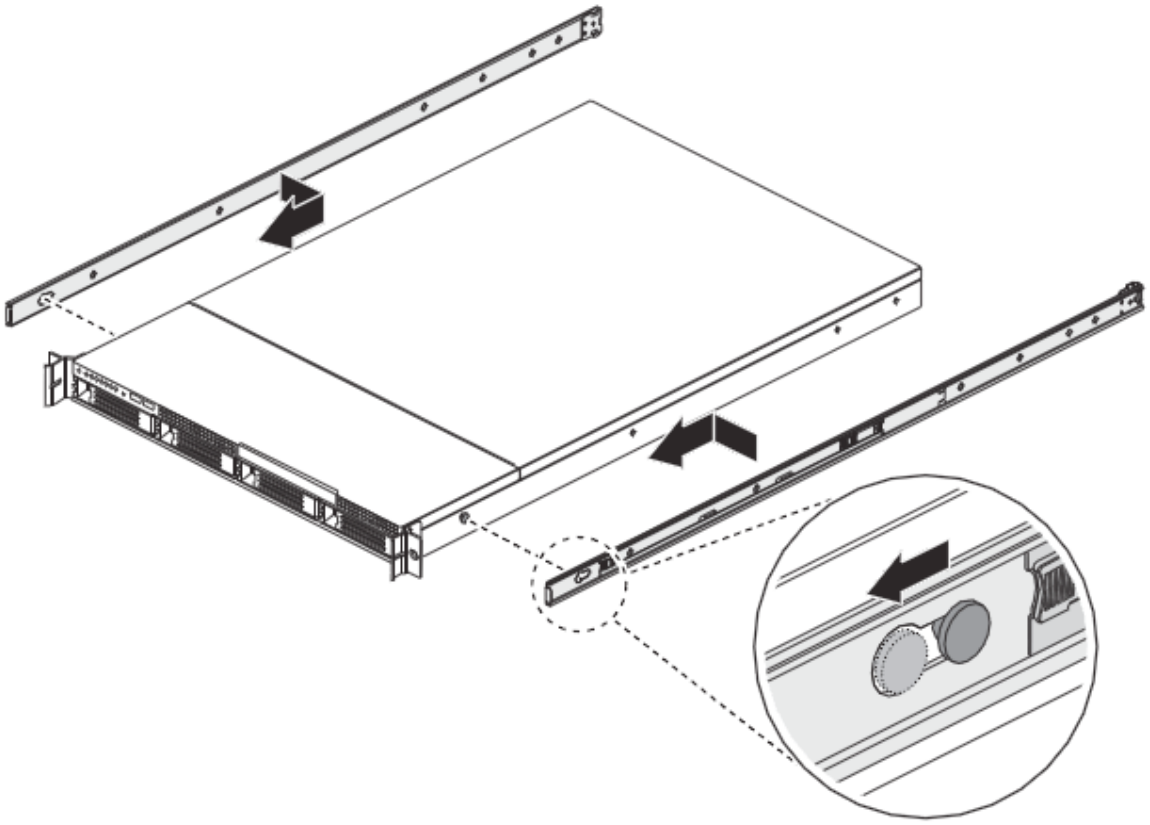


3. Remove the inner rail from the slide rail assembly. Pull out the inner rail, and then pull the release tab to remove it from the rail assembly.

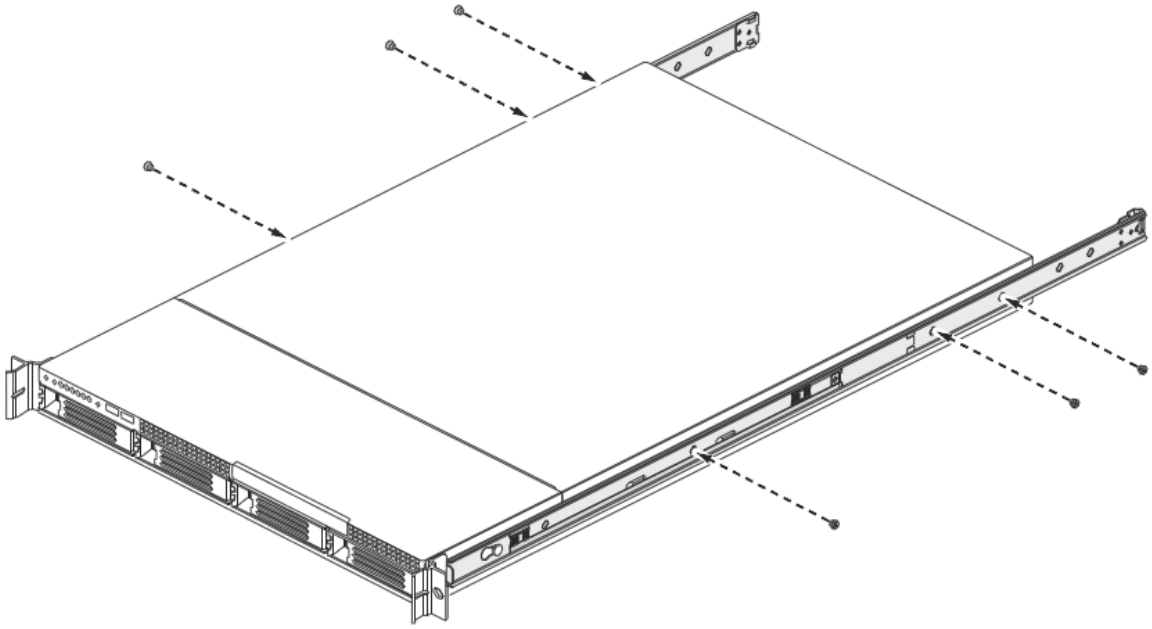




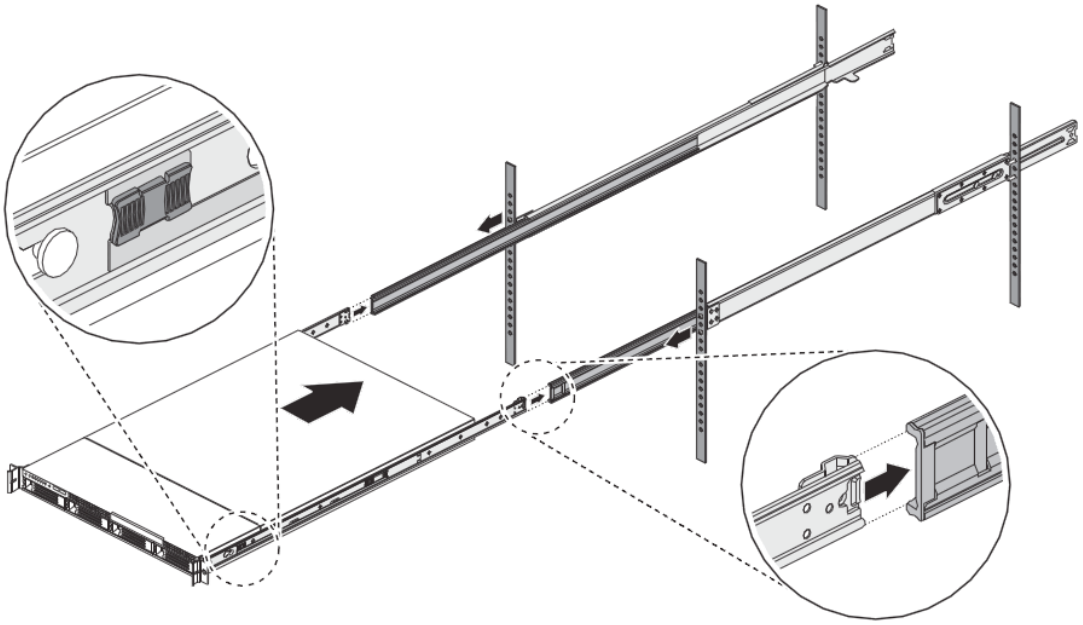
4. Align the inner rail with the protruding rivet head, and then push the inner rail towards the front of the enclosure. The inner rail should snap fit to the side of enclosure.



5. Secure the inner rail to the side of enclosure using 3 included flathead screws. Repeat the above process to install another inner rail to the right hand side of the enclosure.



6. 6-1. Make sure the middle rails are pulled to the front.
   6-2. Lift the enclosure into position and then insert the tips of the inner rails into the entrance point on each of the middle rails.
   6-3. Slowly move the enclosure in to engage the inner rails with the slide rail assembly.
   6-4. When slided half way, the rail lock will engage. Press the release tabs on both sides to slide the enclosure into rack cabinet.

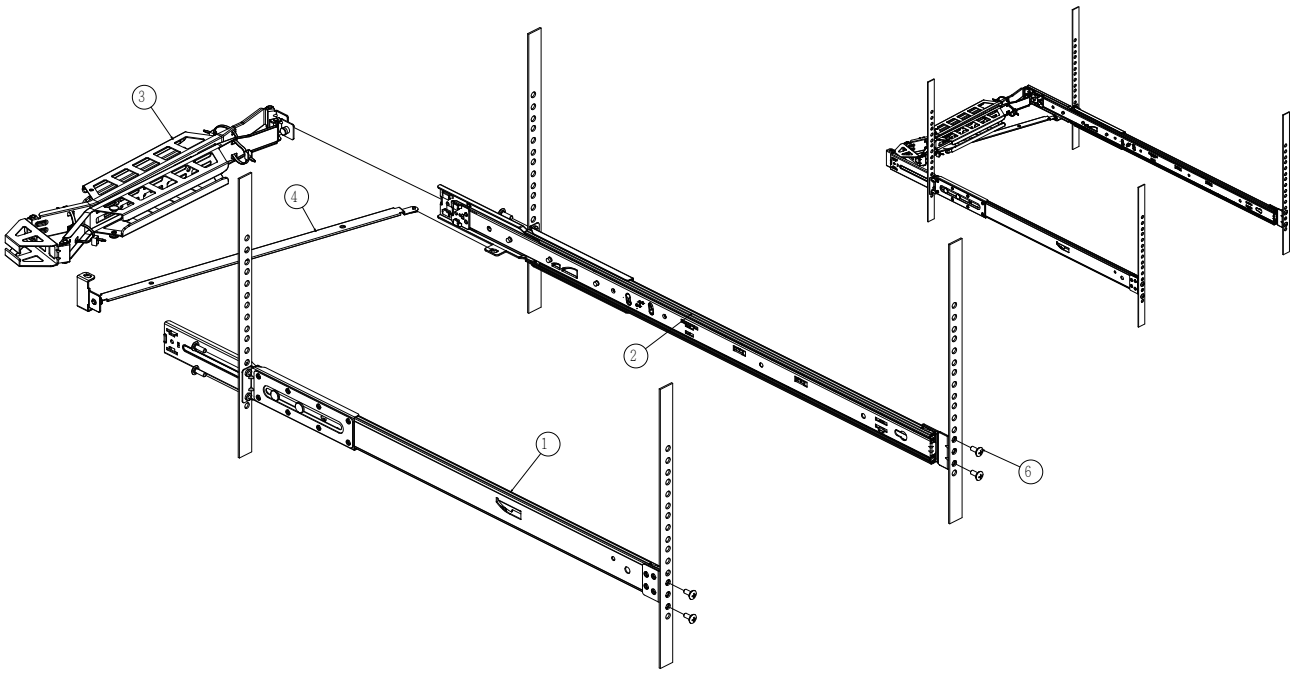


2.4 Hardware Installation - Rackmount Enclosures (12600U & 12620U)

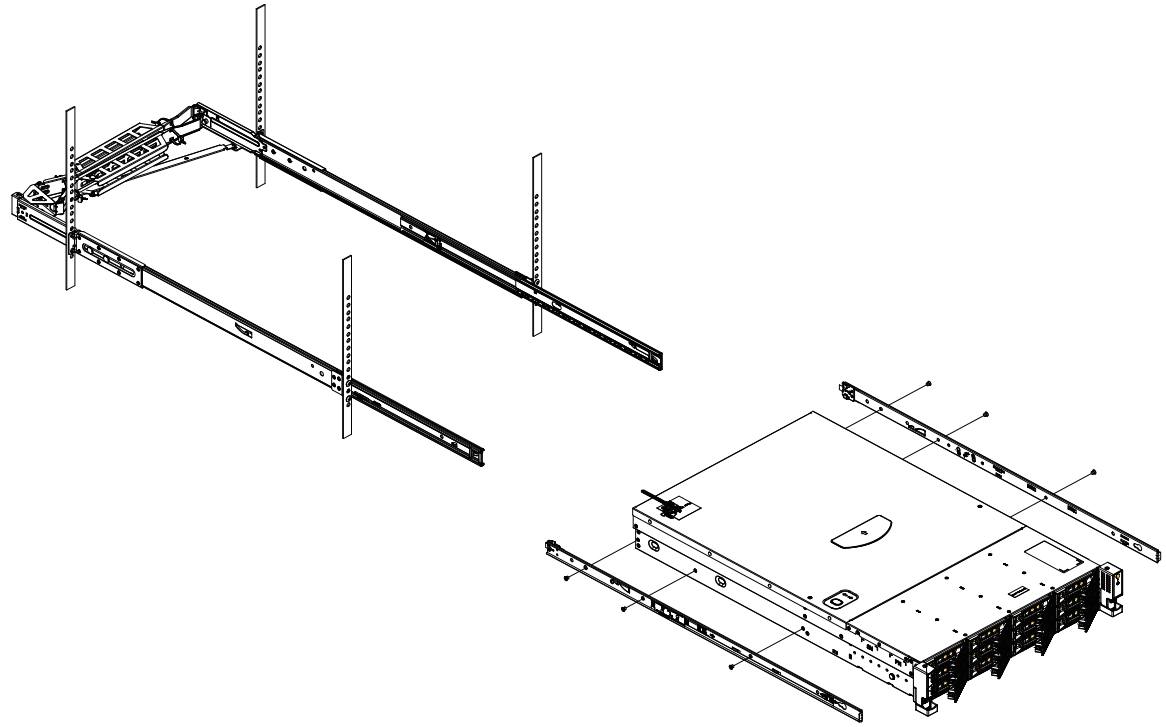
The mounting holes and installation methods are identical for the rack-mount models 12600U and the 12620U.

Follow the procedure to install a 2U rackmount enclosure to a rack cabinet:

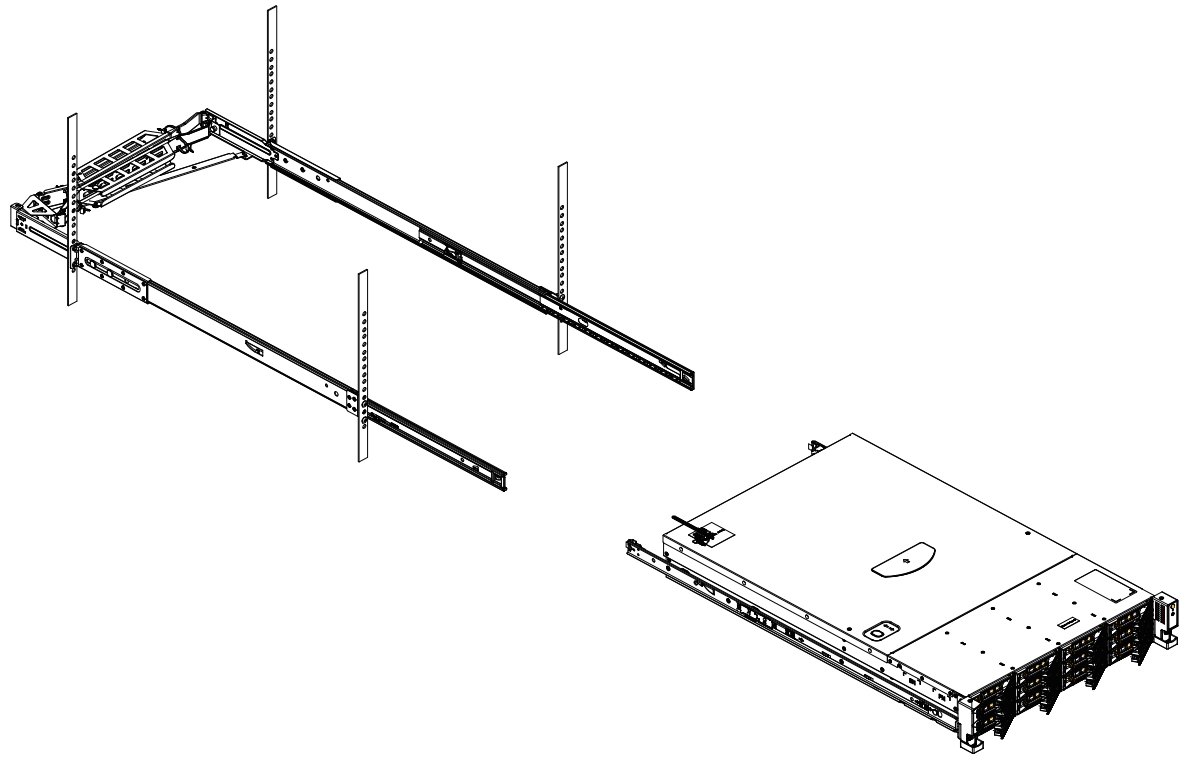
1. Attach the inner and middle rails to the rack cabinet. See previous description.
2. Attach the cabling management arm to the rear of the slide rail assembly.



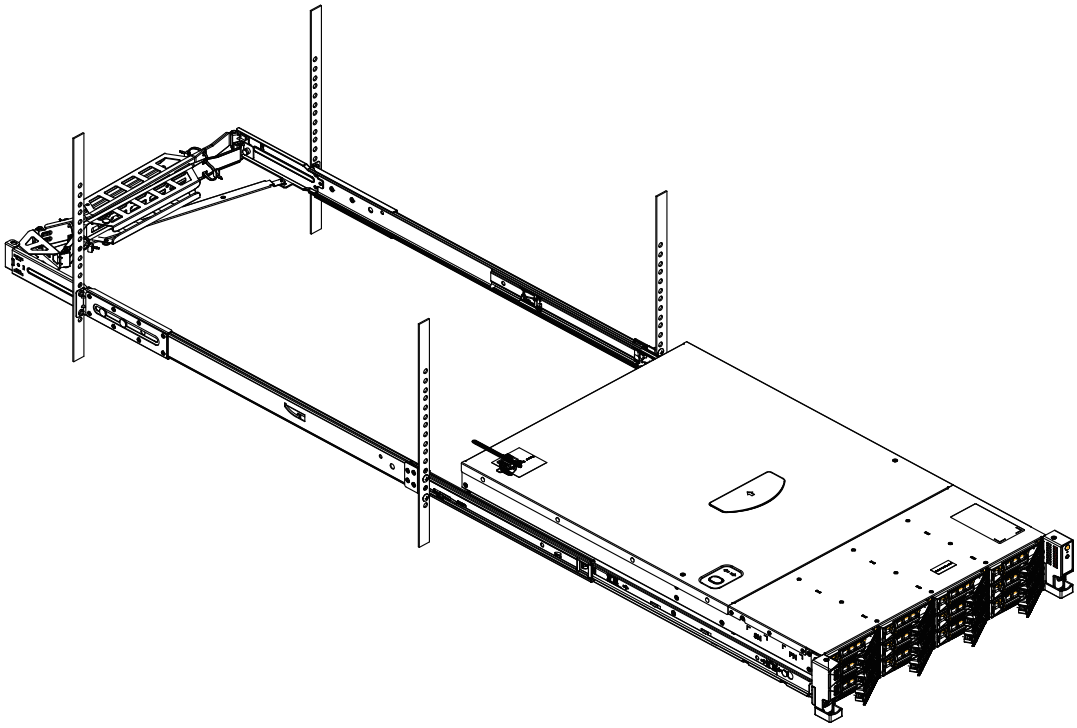
3. Attach the inner rails to the sides of the chassis.



4. Gradually slide the chassis into rack.



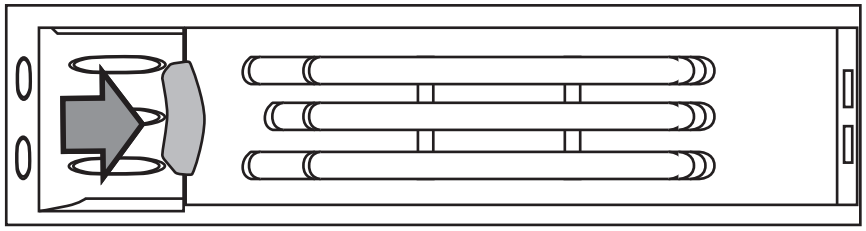
5. Engage the tips of inner rails with that already installed on the cabinet. Push the chassis into the cabinet.



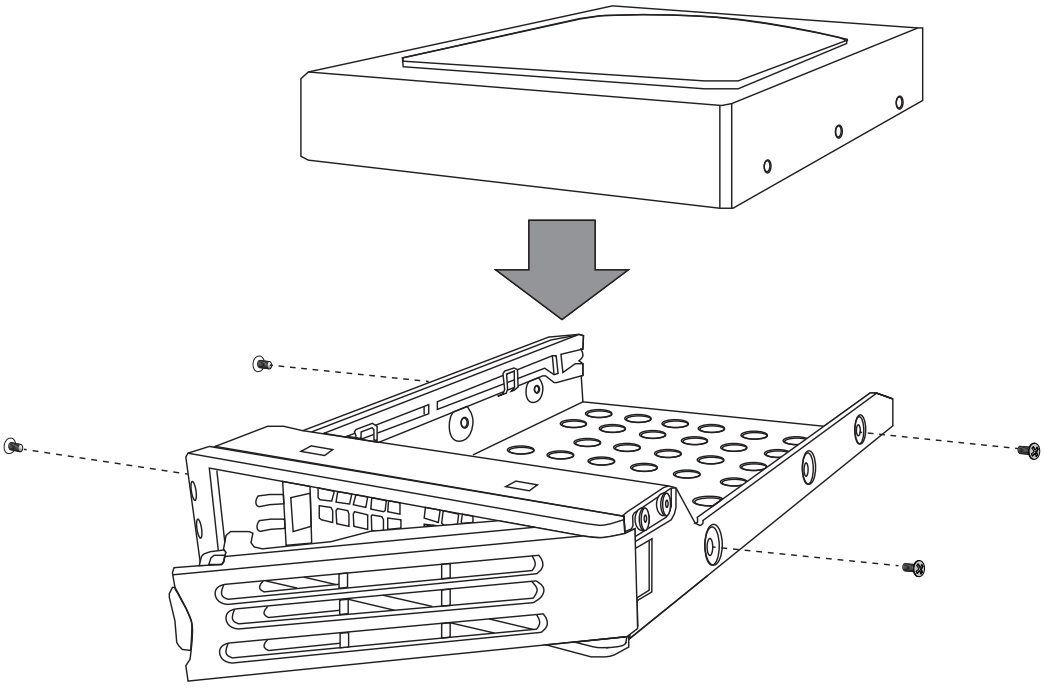
2.4 Installing Disk Drives - 4600U, 12600U and 12620U

Follow the procedure to install a rack mount enclosure:

1. Remove a HDD tray from the server by press the release tab.

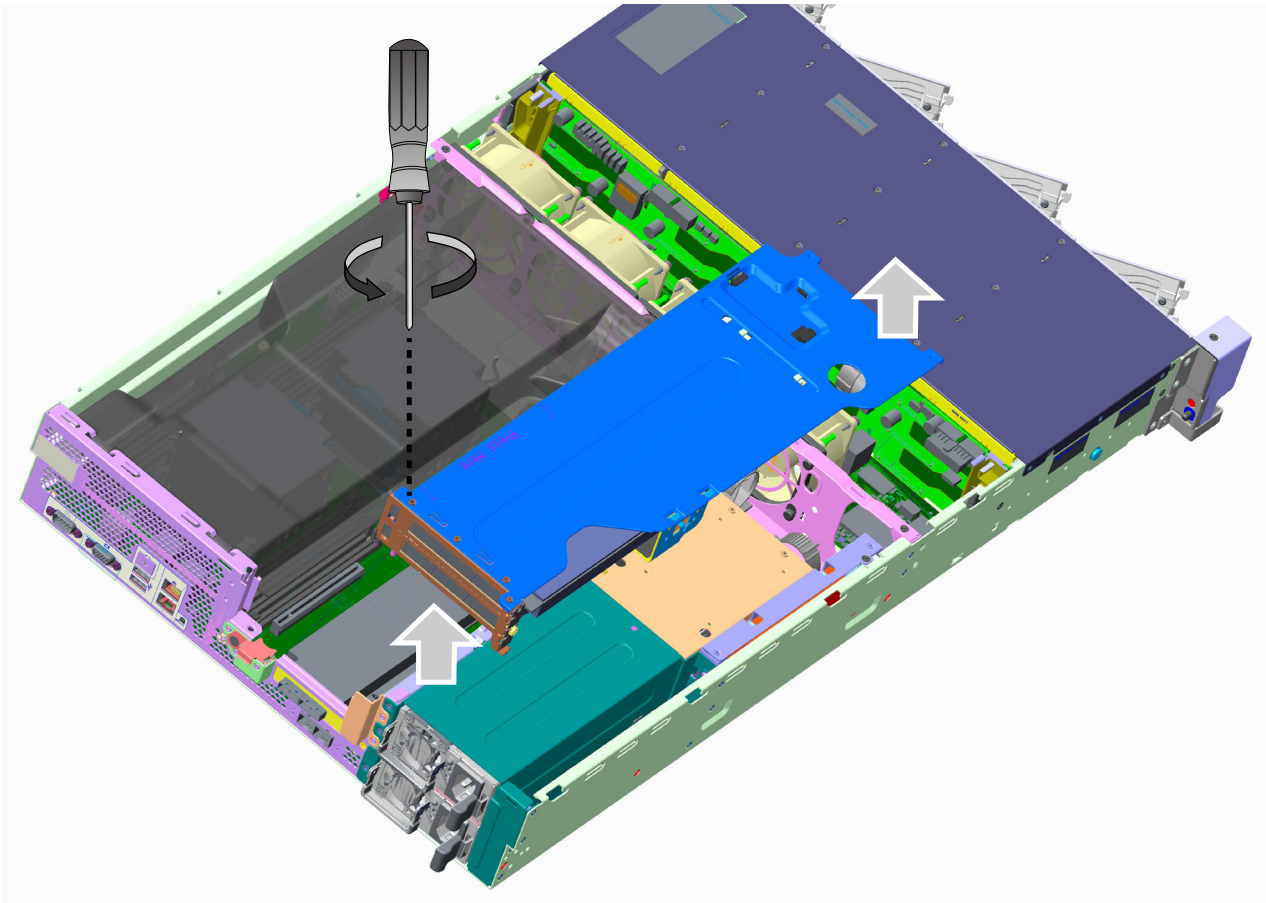


2. Secure and mount a hard disk onto the HDD tray using four screws from the sides of the tray.
3. Insert the HDD tray back in the server. Make sure the lever of the HDD tray is properly in place.



4. Repeat Step 1 to Step 3 if necessary for the other HDD tray.
5. Install rack mounting handles at both side of the NAS server.
6. Install the NAS server in the rack.(Refer to previous discussions)
7. Connect your NAS server to the network with LAN cable from the LAN port located at the back of your NAS server.(At least one network connection is required)
8. Plug the power cord into the power connector on you NAS server.
9. Make sure the power switch on the power supply is in on position.
10. Press the power button on left of the front panel on NAS server.

2.5 Optional PCI-E adaptor installation (Only for 12600U & 12620U)



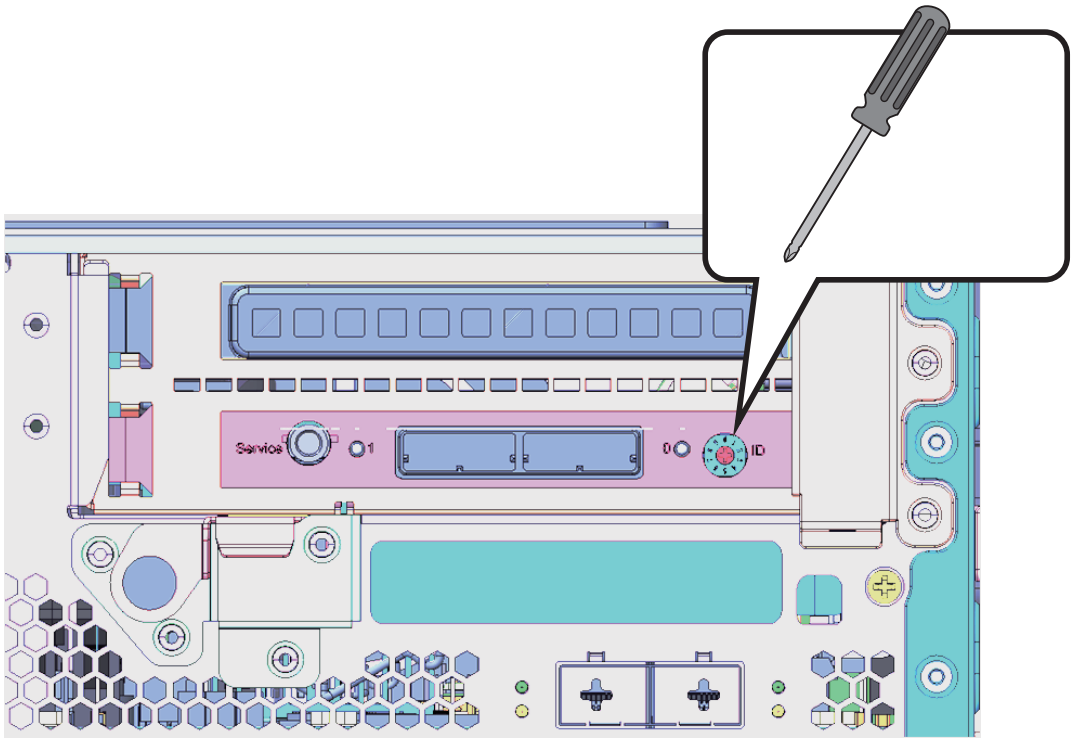
1. Turn off your NAS server and unplug power from the wall.
2. Open the server case.
3. Loosen the screws and remove the riser card support bracket.
4. Place the adapter, component-side down, and press the adaptor firmly into one of the PCI-E slot on the riser card.
5. Tighten the screw for the adaptor.
6. Reinstall the riser card support bracket and make sure that the riser card is fully seated in the PCI-E slot on the main board.
7. Tighten the screw for the riser card support bracket.
8. Close your server case and plug in your power cable.
9. Turn on the NAS server.
10. New PCI-E adaptor is now installed.

Note that only the PCI-E cards certified by Ingrasys can be installed into chassis. Please consult our availability list or website updates for details.

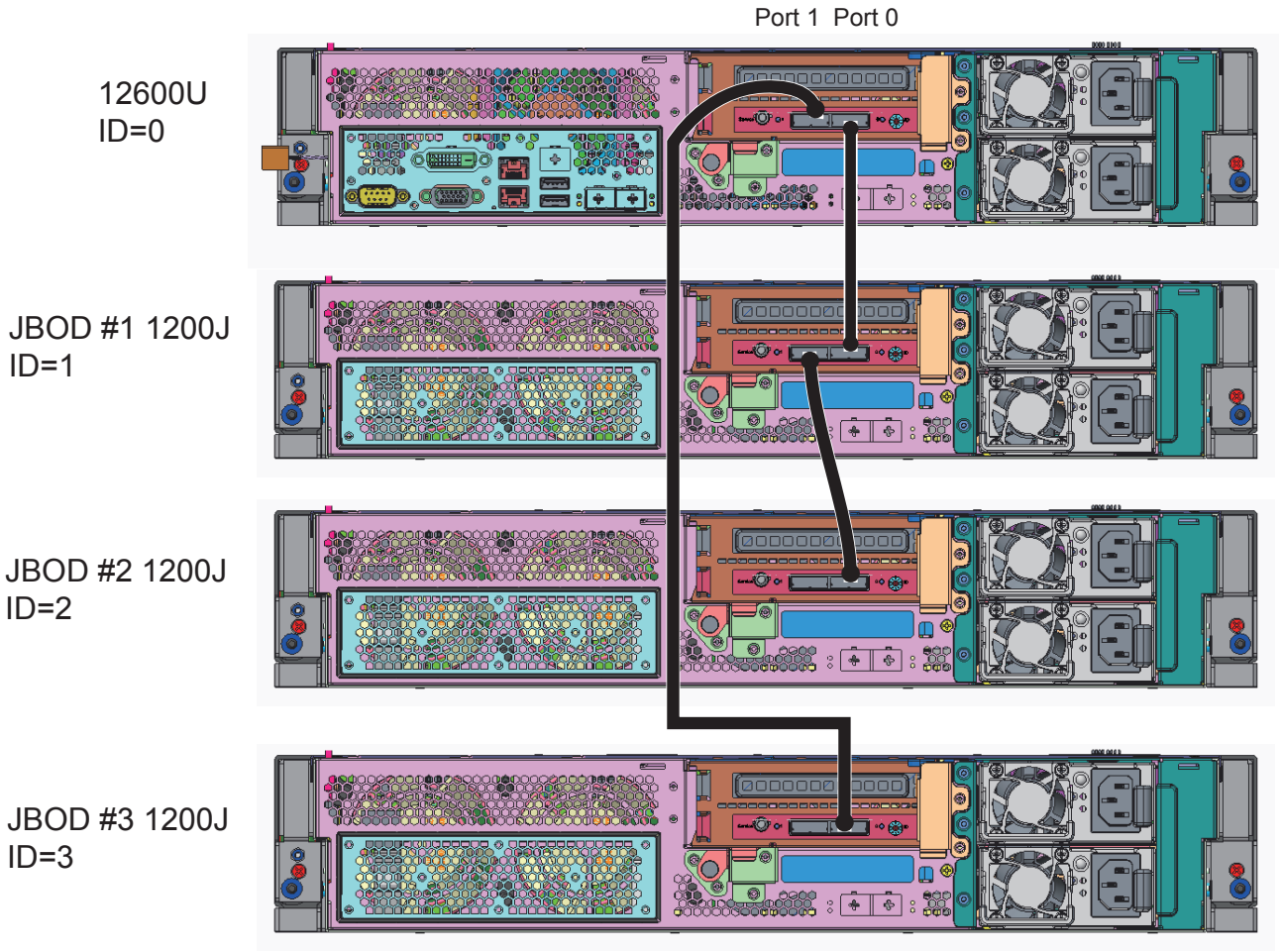
2.6 Connecting Expansion Enclosures (for 12600U & 12620U)

1. To connect expansion enclosures (the 1200J) to the 12600U NAS, first use a small-size Phillips screw to set up the enclosure IDs. These IDs are necessary to address the WWN addresses for the hard disks inside the expansion enclosures.

   Set the NAS server ID to 0, and the IDs on the JBOD enclosures consecutively. The configuration supports up to 3 JBODs.



2. Connect cables between enclosures as shown below. Also make sure the enclosure IDs are properly configured.



IMPORTANT:

1. For the 12620U model, there is no ID switch. The chassis has a default ID, #0, and there is no need to change this default ID.

2. Make sure you configure the SAS/SATA expansion chassis ID (JBOD) to numbers other than #0.

2.7 Starting the System

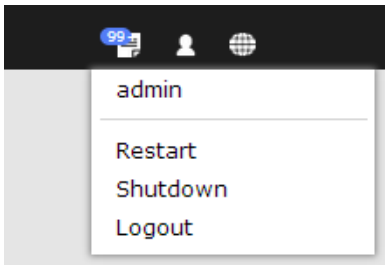
1. Make sure the power switch on the power supply is in ON position.
2. Press the power button -

   Tower - press the button on the front.

   Rack chassis - press the Power button on the left of the front panel of your NAS server. Press the button for longer than 1 second.
3. Wait for the server to boot up. The boot up process takes approximately 5 minutes.

2.8 Shutting Down the System

1. Shut down the system pressing the power button once. The whole shutdown process might take seconds or minutes until data can all be safely distributed to disk drives.
2. To shut down the server from the management page you can find the button on the upper right of the NASFinder screen.



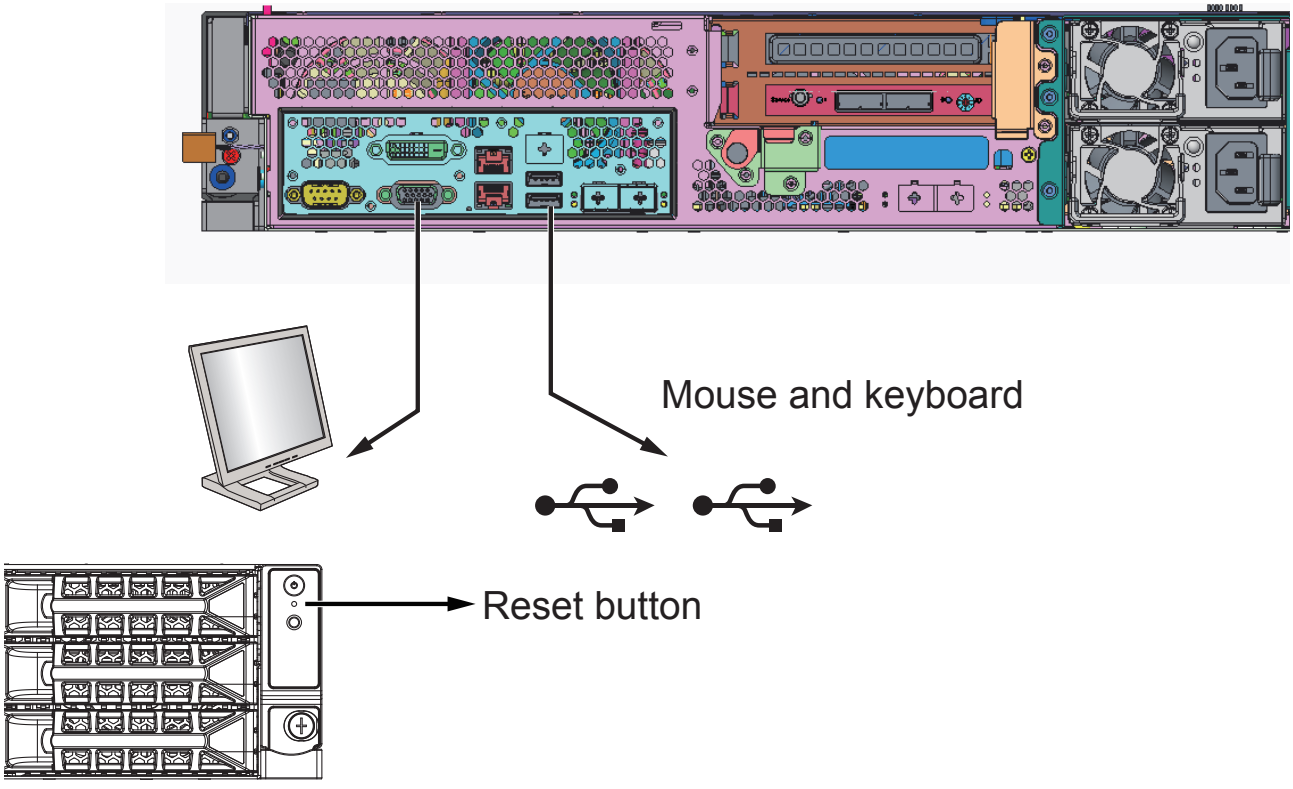
3. To configure automatic power-on and shutdown, you can select System > Maintenance > Reboot/Shutdown on a management console. You can set daily or day in month schedules. See page 64 for more information.

2.9 Drive Tray LED Definitions

LED1 (up) Red	LED2 (down) Blue	Description
Indicator/error	**HDD Access**	
OFF	Lit Blue constantly	No activities on HDD
OFF	Blue blinking	HDD read/write activities
Lit constantly	OFF	Faulty HDD
Red blinking intermittently	OFF	Volume being created or rebuilt
Red blinking rapidly	OFF	Volume has already been exported (unmounted), and is ready for removal.
OFF	OFF	No power or HDD is absent

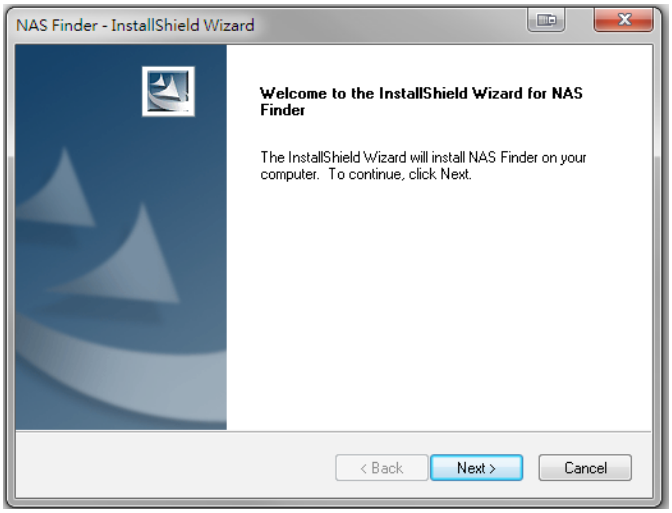
Tips:

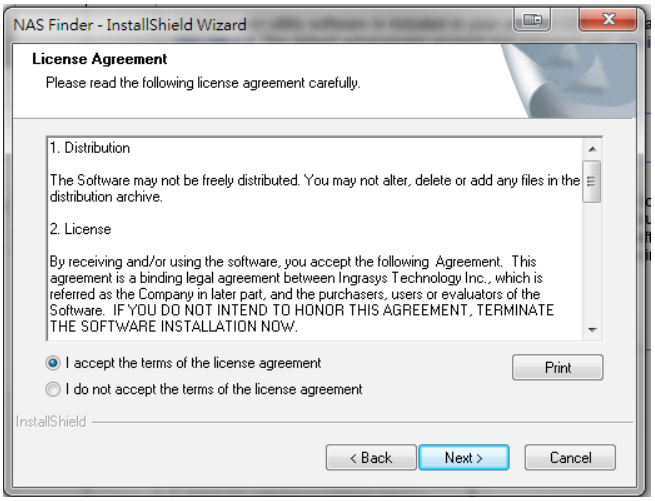
If you lost your access to the 12600 series system, try connect the D-SUB 15 connector to a monitor and a mouse and a keyboard. Try to access the system using the NASfinder. If you still can not access the system, press the Reset button for more than 10 seconds to restore the system defaults especially if the system was re-located, set with a static IP, and connected to a different network. .



2.10 Install the NASFinder Utility

1. A NASFinder utility software is included in your product CD. The default system IP is **192.168.1.1**. The default administrator account and password are: **admin** and **admin**.
2. Install the utility by starting the NASFinder-Setup.exe.
3. Follow the onscreen instructions to install the software.

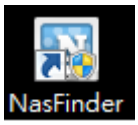

NAS Finder - InstallShield Wizard
Welcome to the InstallShield Wizard for NAS Finder
The InstallShield Wizard will install NAS Finder on your computer. To continue, click Next.
< Back
Next >
Cancel


NAS Finder - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
1. Distribution
The Software may not be freely distributed. You may not alter, delete or add any files in the distribution archive.
2. License
By receiving and/or using the software, you accept the following Agreement. This agreement is a binding legal agreement between Ingrasys Technology Inc., which is referred as the Company in later part, and the purchasers, users or evaluators of the Software. IF YOU DO NOT INTEND TO HONOR THIS AGREEMENT, TERMINATE THE SOFTWARE INSTALLATION NOW.
I accept the terms of the license agreement
I do not accept the terms of the license agreement
Print
InstallShield
< Back
Next >
Cancel

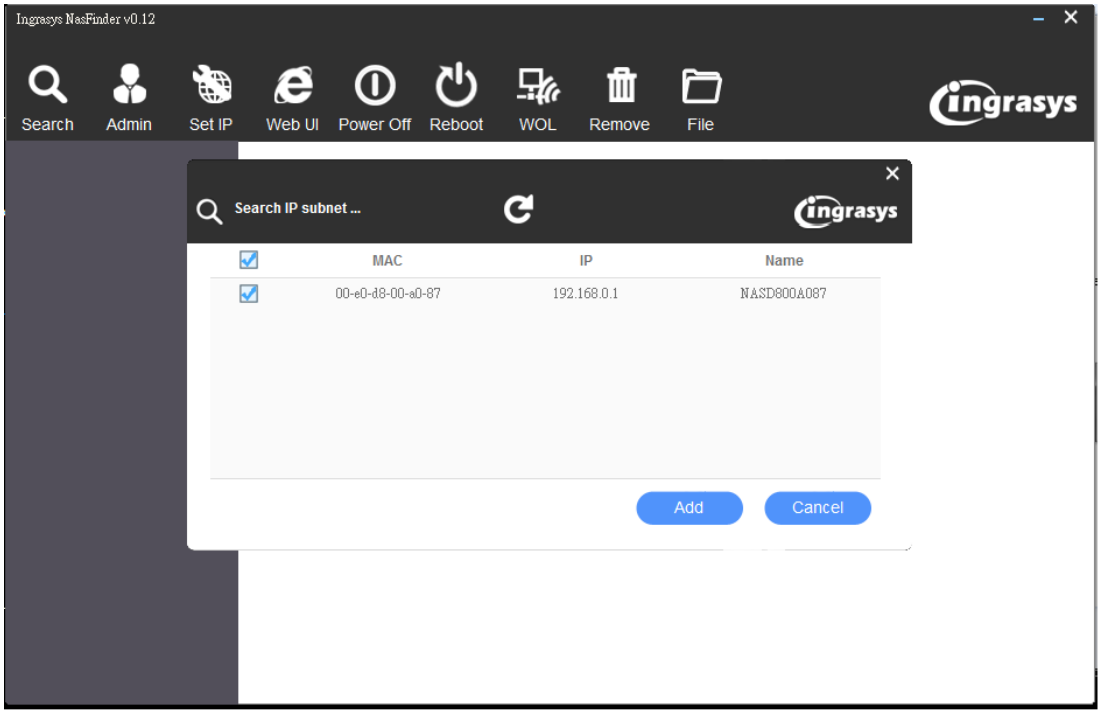
Tips:

If you are prompted to install plug-ins or allowance to execute the program when installing the software, follow the prompts to accept the installation.

4. A desktop icon will be placed. Double-click on it to start the program.

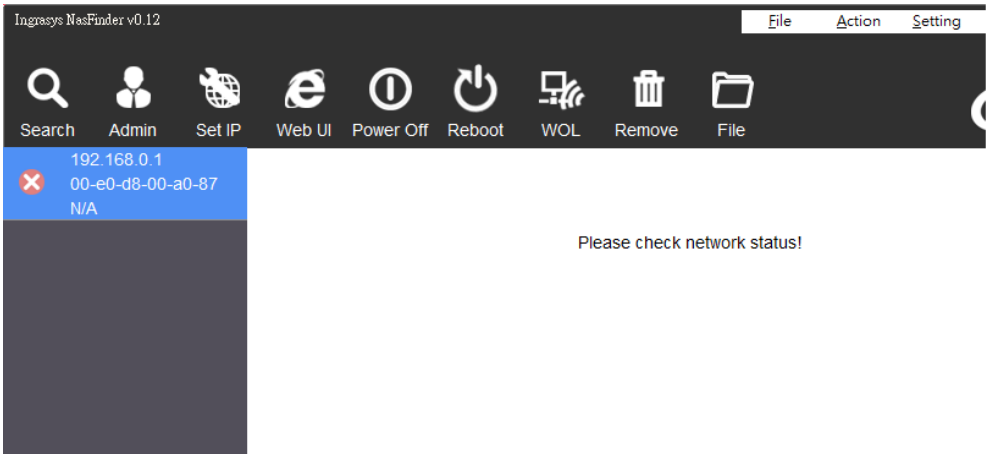


5. After a brief search, the NAS server will be listed with its MAC address, IP, and server name shown on the screen. Click to select its checkbox.



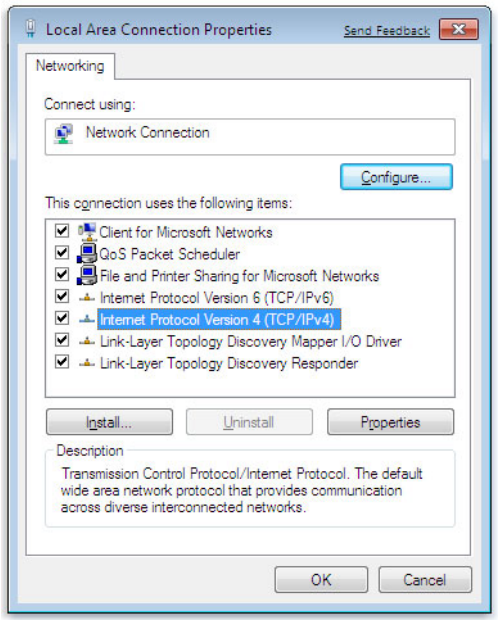
NOTE:

The NAS server comes with a default IP, <192.168.1.1>. If your router or other network devices are using the same IP address, an error message will appear.



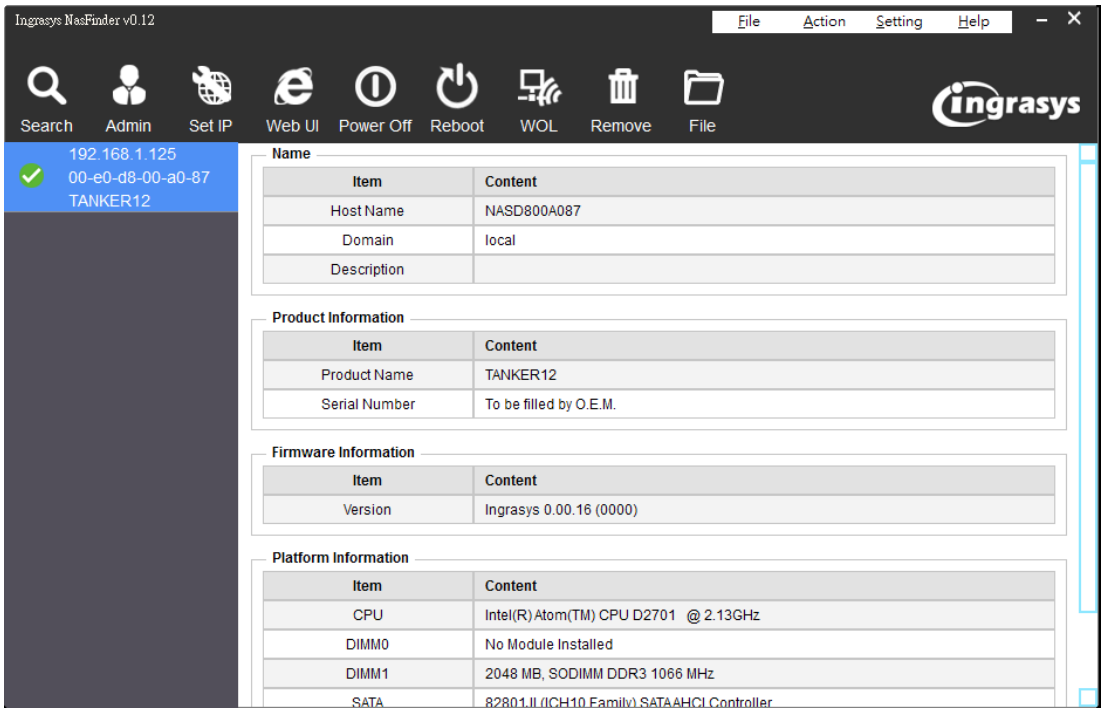
If this condition occurs,

1. Stop the system by pressing the Power button.
2. Connect the LAN cable directly to your PC's LAN port.
3. Configure your PC's IP address to 192.169.1.X, to the same subnet.
4. Open a browser session with the NAS server using the 192.168.1.1 address.
5. Change the NAS server's IP address, or, change the networking setting to DHCP.

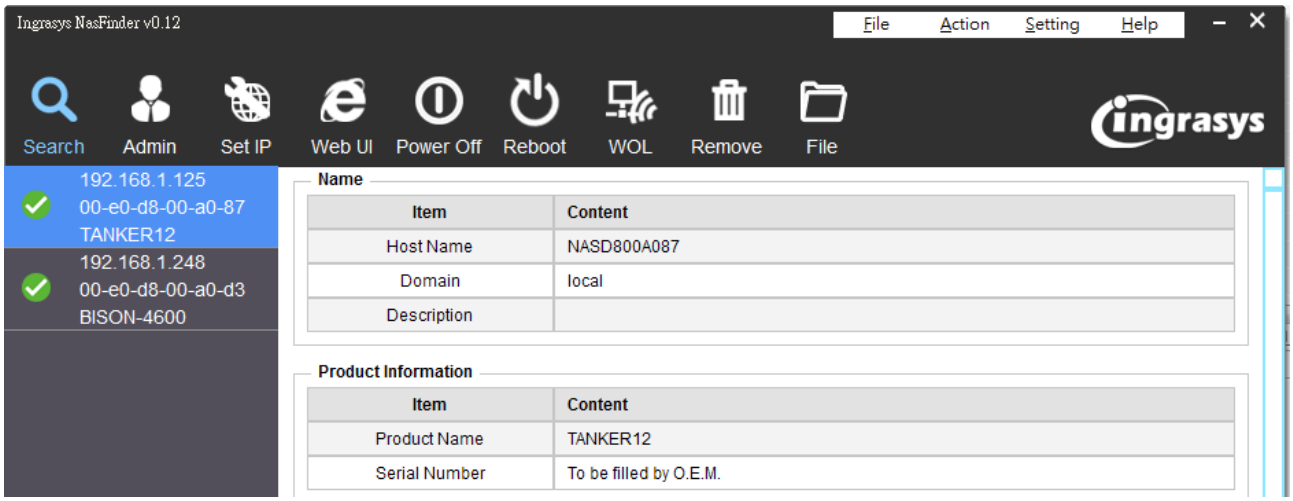


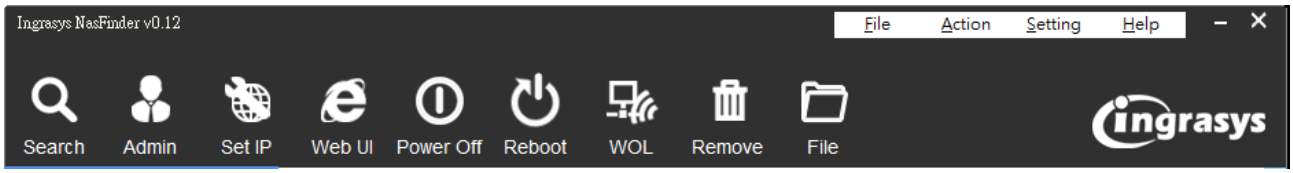
6. After the change to listening to a DHCP server, you need to connect the cables to a network switch or router where a DHCP server is present. Make sure your DHCP server is up and running and can be reached by both the network switch and the management computer.

7. Click the **Add** button to enlist the NAS server found in your subnet. The basic information of the connected server will be listed: including that of Host name, Domain, Product name, Serial number, firmware rev. no., and so on.



If there are multiple NAS servers in your network, you can select the checkboxes in front of them and enlist them into the management queue.





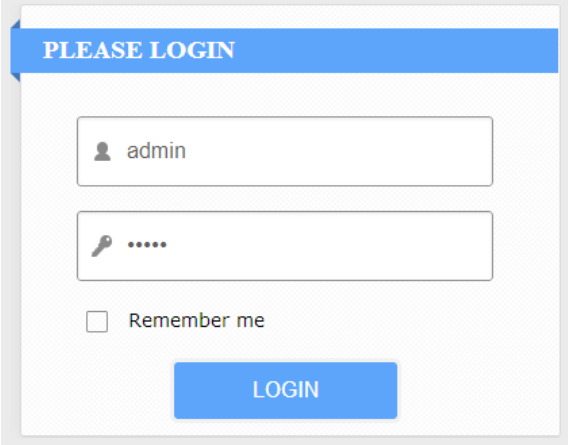
The basic functions of the NASFinder are described as follows:

Search	Click to poll the presence of NAS server(s) in your local network.
Admin	Allows you to change the Admin account and password.
Set IP	Allows you change the static IP for a NAS server.
Web UI	Opens a web console with the NAS server. You may also open a web browser and enter the NAS server's IP address in the URL field to open a web console.
Power Off	Power down the selected NAS server.
Reboot	Reboots the selected NAS server.
WOL	Wake on LAN. Uses this button to remotely power up a NAS server via network connections.
Remove	Removes a detected NAS server from the managed queue.
File	Opens up a Folder Group in a network share.

NOTE:

Admin is a built-in administrator account. It is like the root account in UNIX or the administrator account in Windows 7. Using this account, users have access to the administration homepage and all the storage resources. By default, the password for this user account is "admin." To prevent unauthorized access, it is highly recommended to change the password after the initial setup.

You can access the management GUI by clicking on the Web GUI button. Enter "admin" and "admin" as the user name and password at the initial startup.



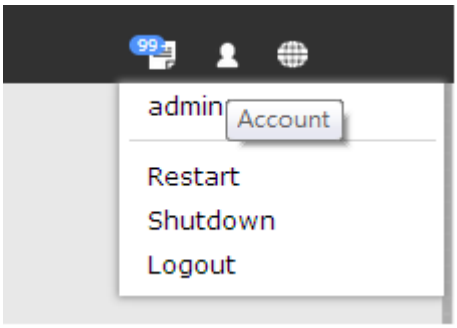
You may also key in the **"http://<IP address>/admin/zf/public/"** in your browser's URL field to start a management session.

NOTE:

Once you logged in and left your web console unattended for 5 minutes, the server will require you to log in again the next time you access the web console to prevent unauthorized access.

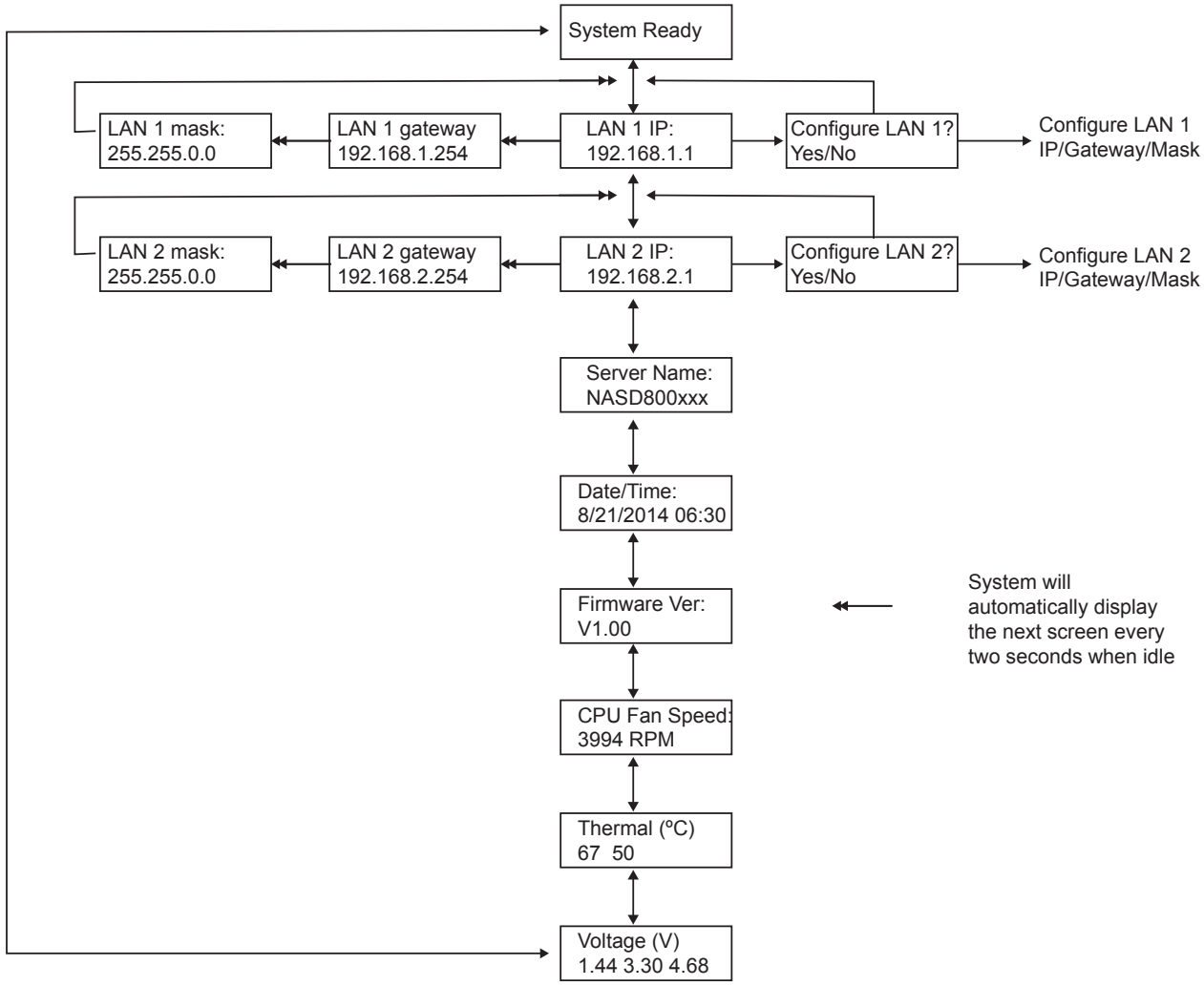
2.11 Using the Top Screen Tools

1. **Event**: Click on the Event button to display the Event window, which lists recent events.
2. **Account**: Click on the Account button to display the **Restart**, **Shutdown**, and **Logout** commands. A confirm box will prompt for reassurance of command execution.
3. **Language**: Click to select a supported language for all captions and texts in the management GUI interface.



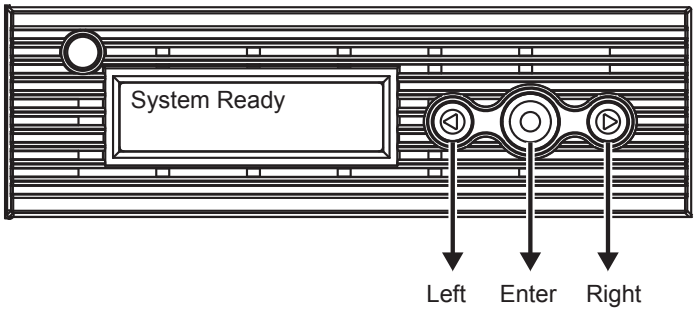
2.12 Configuring IP Address Using the LCD Keypad (Tower 4600T Only)

LCD menu console flowchart

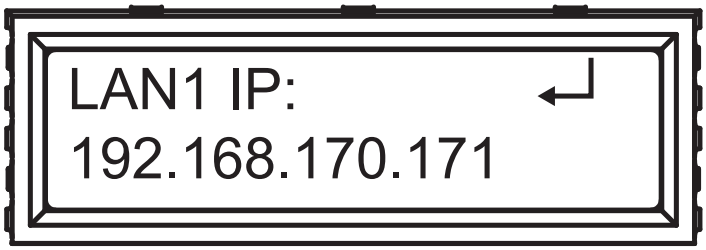


Configuring IP address using the LCD console.

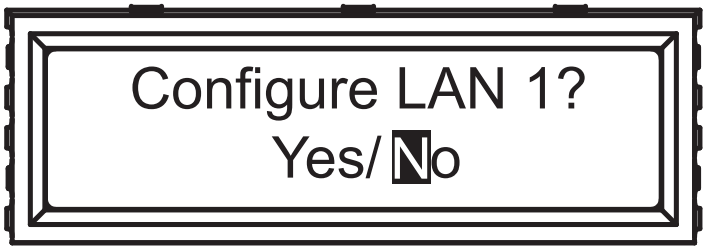
1. After the server boots up, the LCD console displays System Ready. Press the right button.



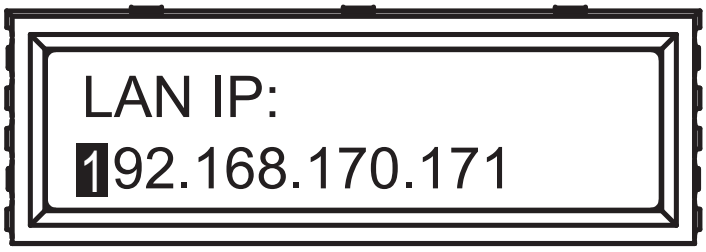
2. The IP address of LAN 1 is shown. Press the Enter button to configure its IP address. Note that the ↵ symbol on the upper right corner indicates that the IP address can be configured using the LCD console.



3. Move the cursor to Yes using the left/right buttons and then press the Enter key to confirm.



4. Move the cursor to the correct position using the left / right buttons. Then press the Enter key to change a number.



5. After you edit the last digit of the IP address, press the right button and configure the Subnet Mask address.

6. Repeat Steps 4 to Steps 5 to configure the Subnet Mask and Gateway address.

7. After you edit the last digit of the Gateway address, press the right button. Move the cursor to Save and save the setting or Edit to repeat the above process or Abort to quit the configuration process without saving.

7. After you edit the last digit of the Gateway address, press the right button. Move the cursor to Save and save the setting or Edit to repeat the above process or Abort to quit the configuration process without saving.

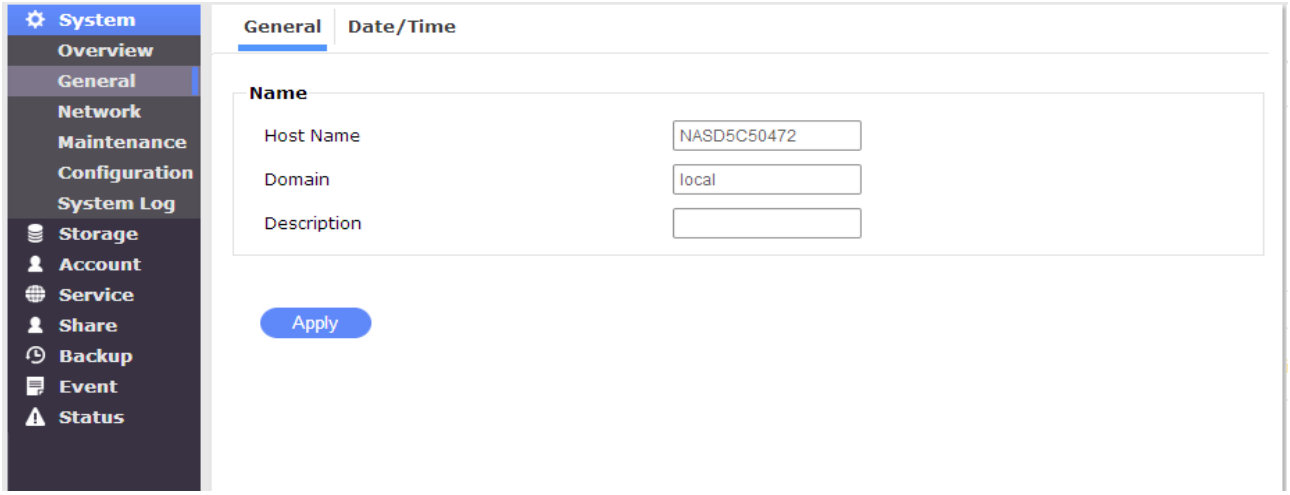
Chapter 3 Managing & Setup: System

The system menu provides access to the system overview, system operating status, network configuration, maintenance, configuration, and system log configuration pages.

3.1. System General Page

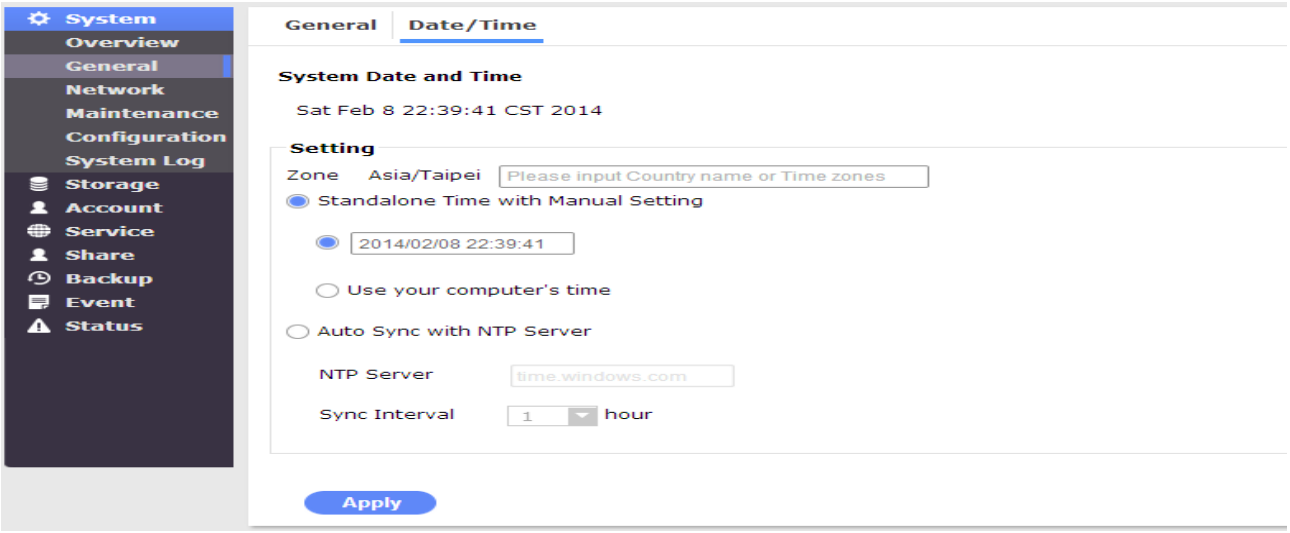
The General page provides access to changing the Host Name, Domain, system description, and a Server Identify function. This page displays on the first log-in.

If you have multiple servers in a location and can not be sure where your server is, use the Server Identify button to light the UID LED.



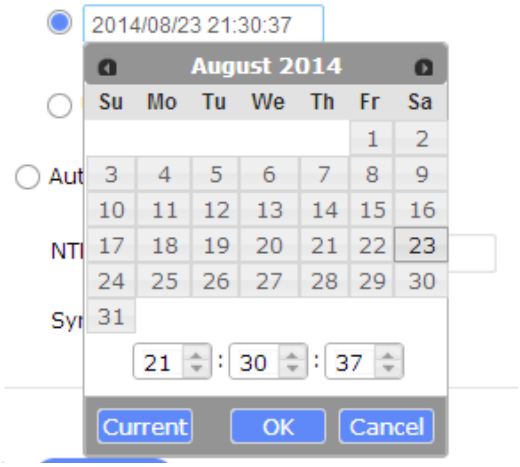
Date/Time

The Date/Time window displays the current system time, and allows you to configure the time zone, and the use of an NTP (Network Time Protocol).



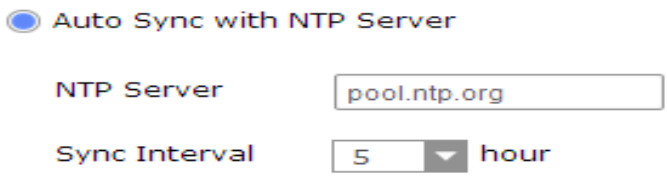
To configure the time zone, click on the empty Etc/UTC entry field. A pull-down menu of all time zones on earth will be available from the pull-down list.

You may then manually configure a time by clicking on the empty entry field or select the check-circle of "Use your computer's time." When doing so, your NAS server's time will be synchronized with that of the PC you use to make a web console.



You can also acquire an accurate time from a time server on the network provided that you have a network connection to the Internet. The default is "pool.ntp.org."

You may then specify the intervals your NAS server synchronize its time with the time server.



3.2. System > Overview

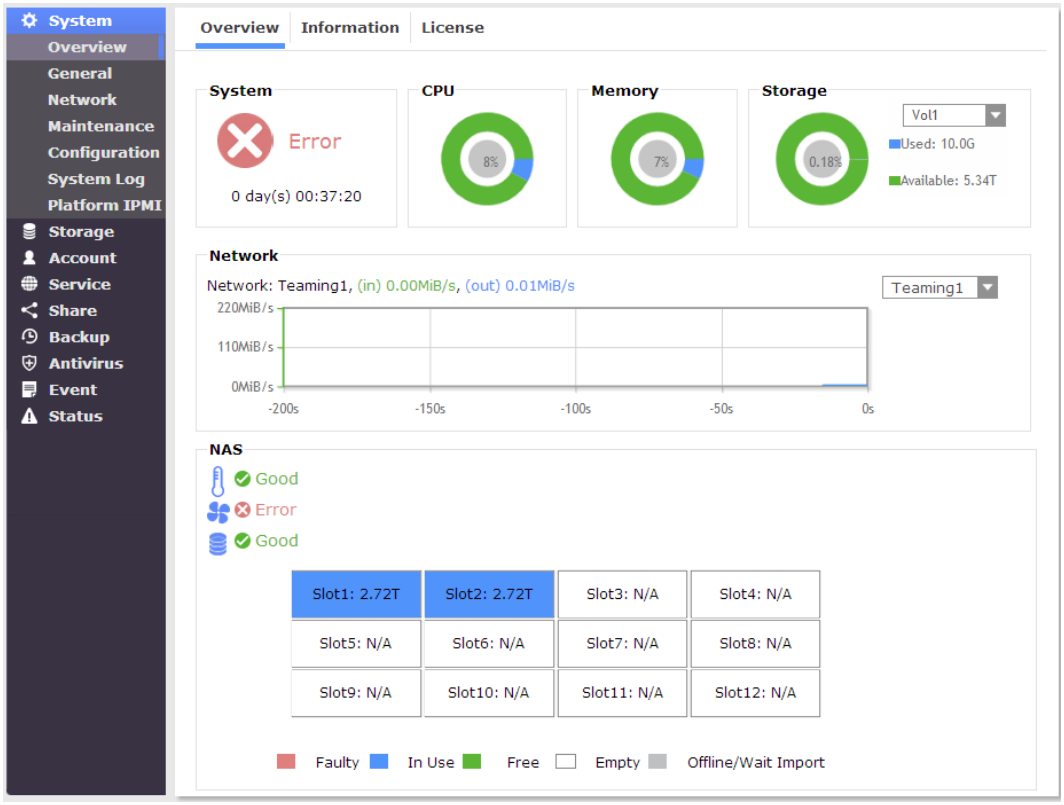
The Overview page provides a glimpse of current CPU and memory resources, network flow, and Storage uses, and the direct access to the working statuses of hard disk drives.

You can also click on the status icons on the lower left of the screen to move to the Status window to get more details of the current operation status.

Thermal events

System errors

Storage events

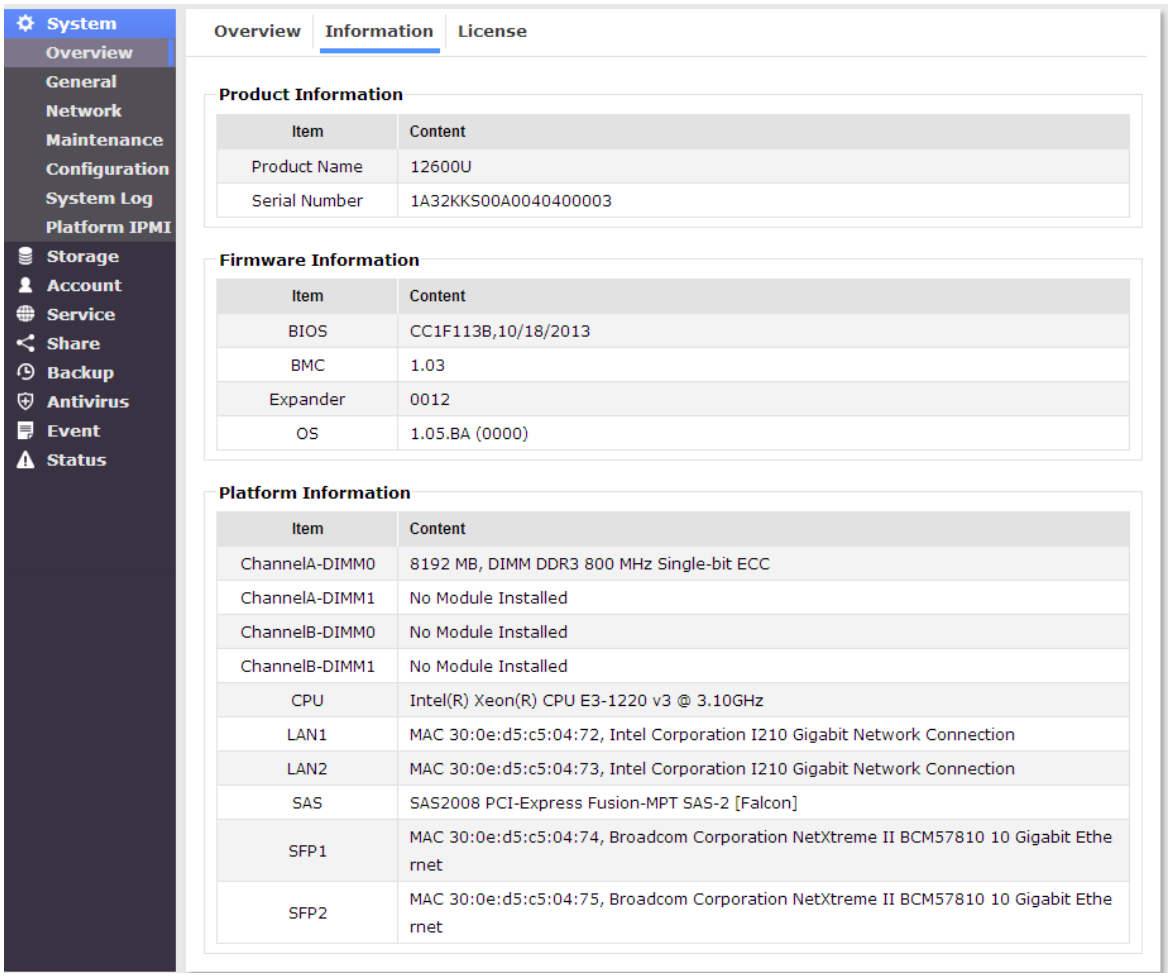


3.3. System > General

Please refer to page 40 for information on the General page.

3.4. System > Network

3.4.1 System > Network > Information

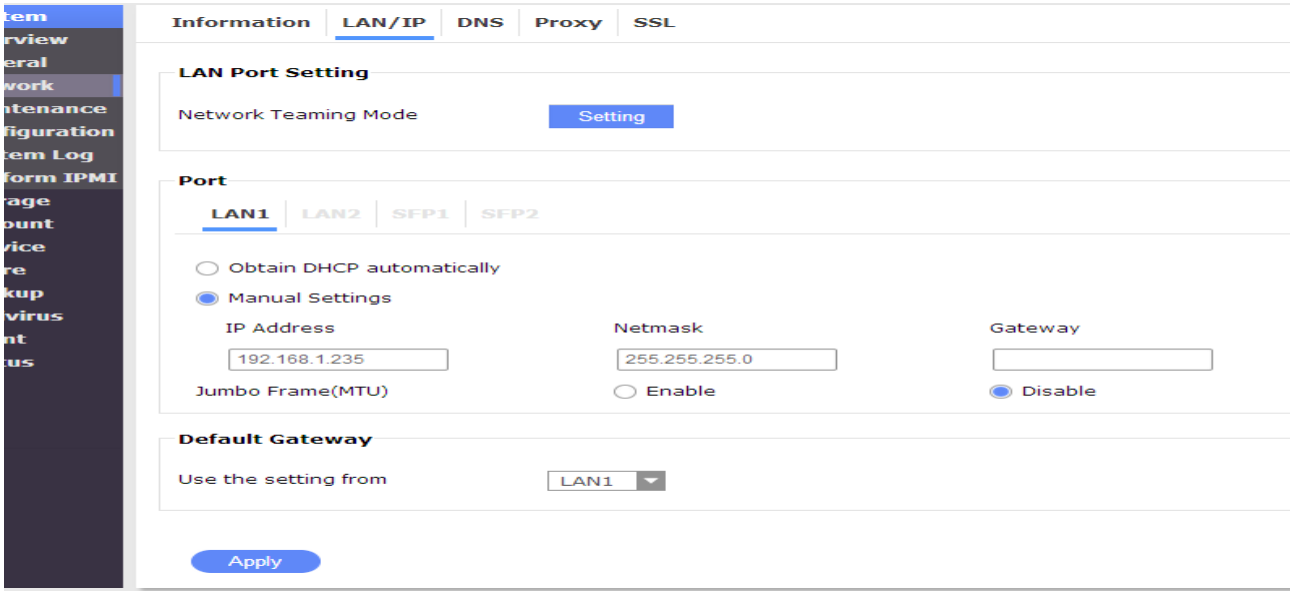


The Network Information page displays the current networking including:

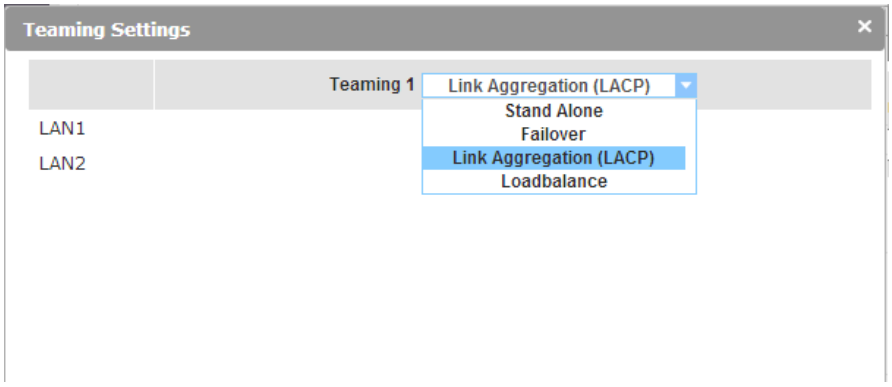
1. Teaming Info: LAN port Link Aggregation setup. See the next section for details.
2. IPv4 and LAN Info: Shows your current IPv4 information, such as IP Address, subnet mask, gateway, MTU, Speed/Mode, and DNS-related information.
3. Server: Shows your current Domain Name server and default gateway.
4. Servers: Displays the servers present in your local and Internet networks, such as the NTP server, WINS server, and HTTP Proxy. A Proxy server is one that acts as an intermediary for requests seeks resources over the network. The Proxy server ficilitates access to contents on the World Wide Web and providing uniform access in a network. Their existence depends on your current network environment.

3.4.2 System > Network > LAN/IP

The Network LAN/IP page provides access to your local network configurations.



1. LAN Port Setting - Network teaming mode:



The Bison series supports IEEE 802.3ad Link Aggregation that enables methods of combining (aggregating) multiple network connections in parallel to increase throughput and provides redundancy in case of single link failures.

Each of the LAN port can be configured into the following operation modes:

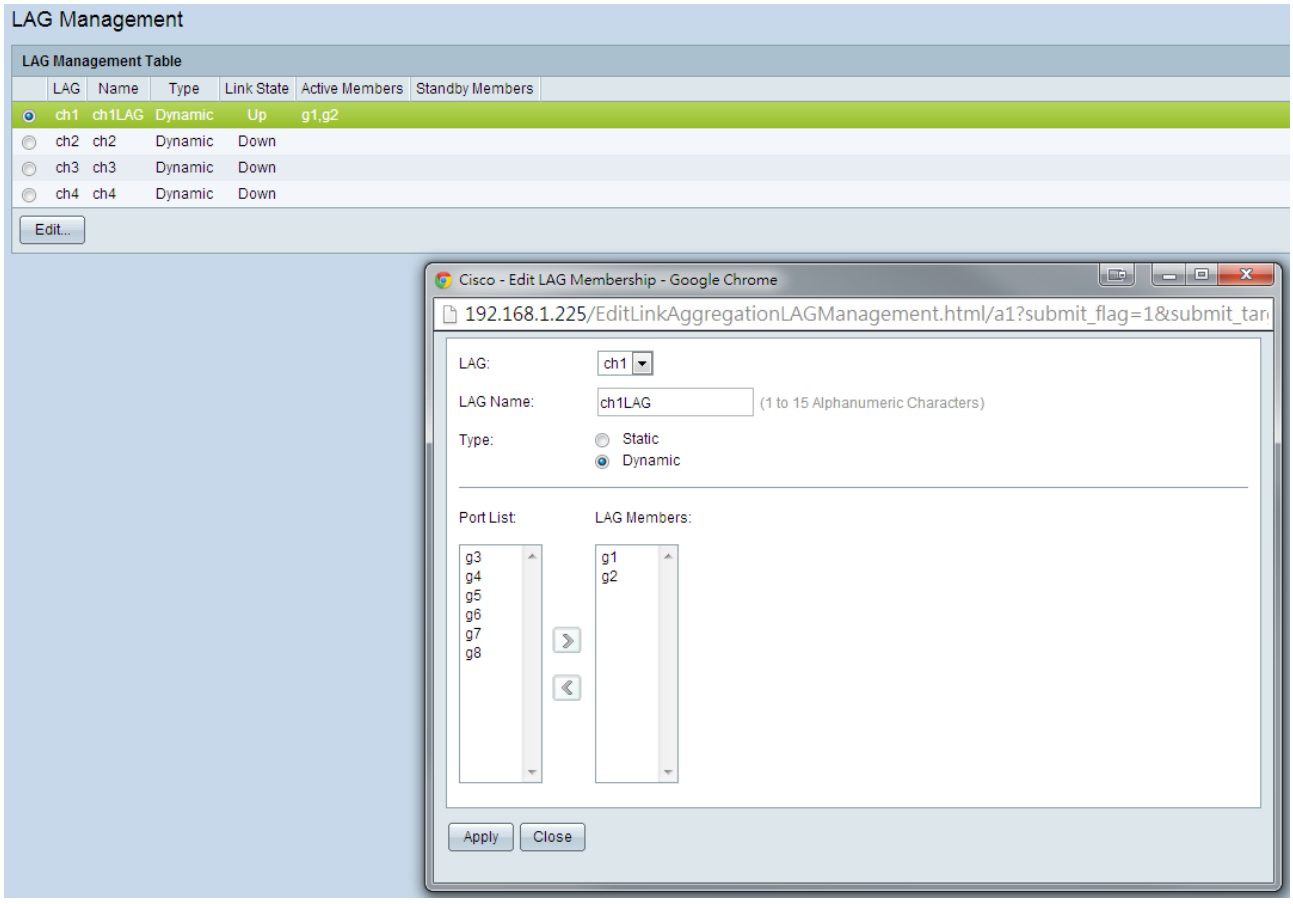
Stand alone - no fault tolerance and no combined throughput.
Failover - two or more LAN ports formed into fault-tolerant team of physical links.

LACP (Link Aggregation Control Protocol) - Combining physical ports together can occur such that multiple interfaces share one logical address (i.e. IP) or each physical address (i.e. MAC address) has its own address.

LACP takes effects by sending frames down all links that have the protocol enabled. If the protocol finds a device on the opposite end of the link is LACP-enabled, frames will be sent over multiple links as if they are transmitted over a single logical link.

Load Balance - Transmit network packets in sequential order from the first available network interface (NIC) slave through the last. This mode provides load balancing and fault tolerance.

Note that corresponding configurations must also be enabled on your network devices, such as a network switch. Shown below is a sample screen from a Cisco network switch.


LAG Management
LAG Management Table
LAG Name Type Link State Active Members Standby Members
ch1 ch1LAG Dynamic Up g1,g2
ch2 ch2 Dynamic Down
ch3 ch3 Dynamic Down
ch4 ch4 Dynamic Down
Edit...
Cisco - Edit LAG Membership - Google Chrome
192.168.1.225/EditLinkAggregationLAGManagement.html/a1?submit_flag=1&submit_tar
LAG: ch1
LAG Name: ch1LAG (1 to 15 Alphanumeric Characters)
Type: Static Dynamic
Port List: LAG Members:
g3 g4 g5 g6 g7 g8
g1 g2
Apply Close

2. Port - **LAN1** and **LAN2**

Obtain DHCP automatically - Acquires an IP address from a DHCP server within your local network. This is not a default, and is configurable after you log in using the default 192.168.1.1 address.

Manual setting -
Select the Manual setting check circle to manually enter a static IP address, network mask, gateway IP address, Jumbo Frame(MTU), and the Wake on LAN options.

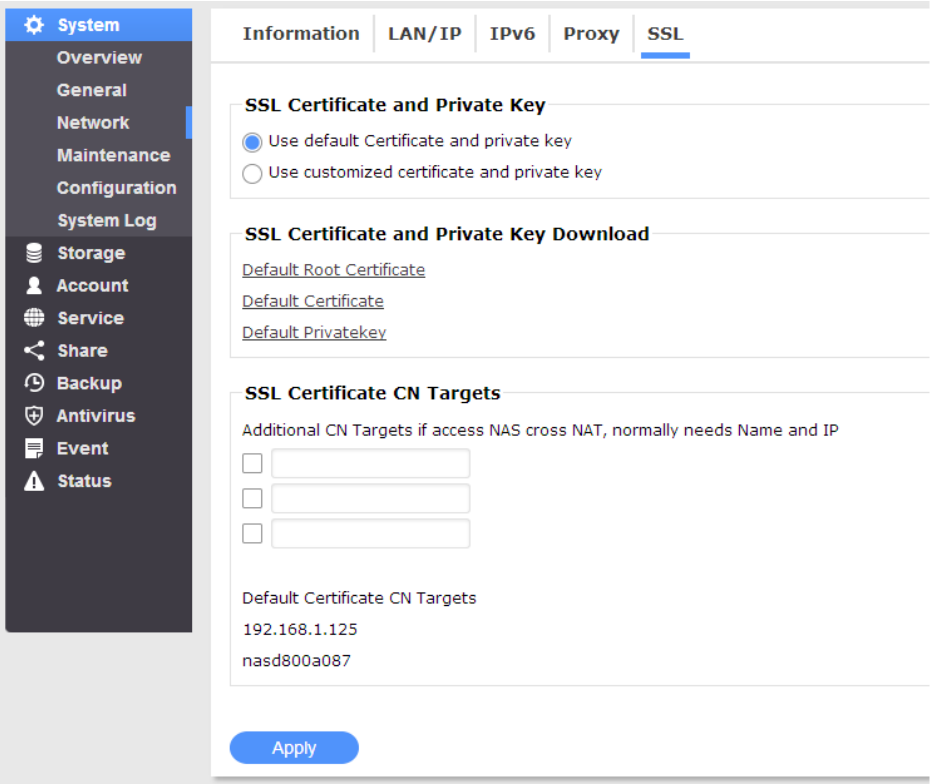
The Jumbo Frame refers to the maximum packet size of up to 9,000 bytes (local network, or, to be compatible with transmission over the Internet, 1,500 bytes).

The Wake on LAN setting (available for the 4600 series only) enables you to power up the server. Wake-On-LAN allows administrators to remotely power on your NAS server to perform maintenance task with no need to go to the server physically.

NOTE:

Only the 4600U/T supports the Wake on LAN function. The 12600U series does not support this function.

3.4.3 SSL Settings

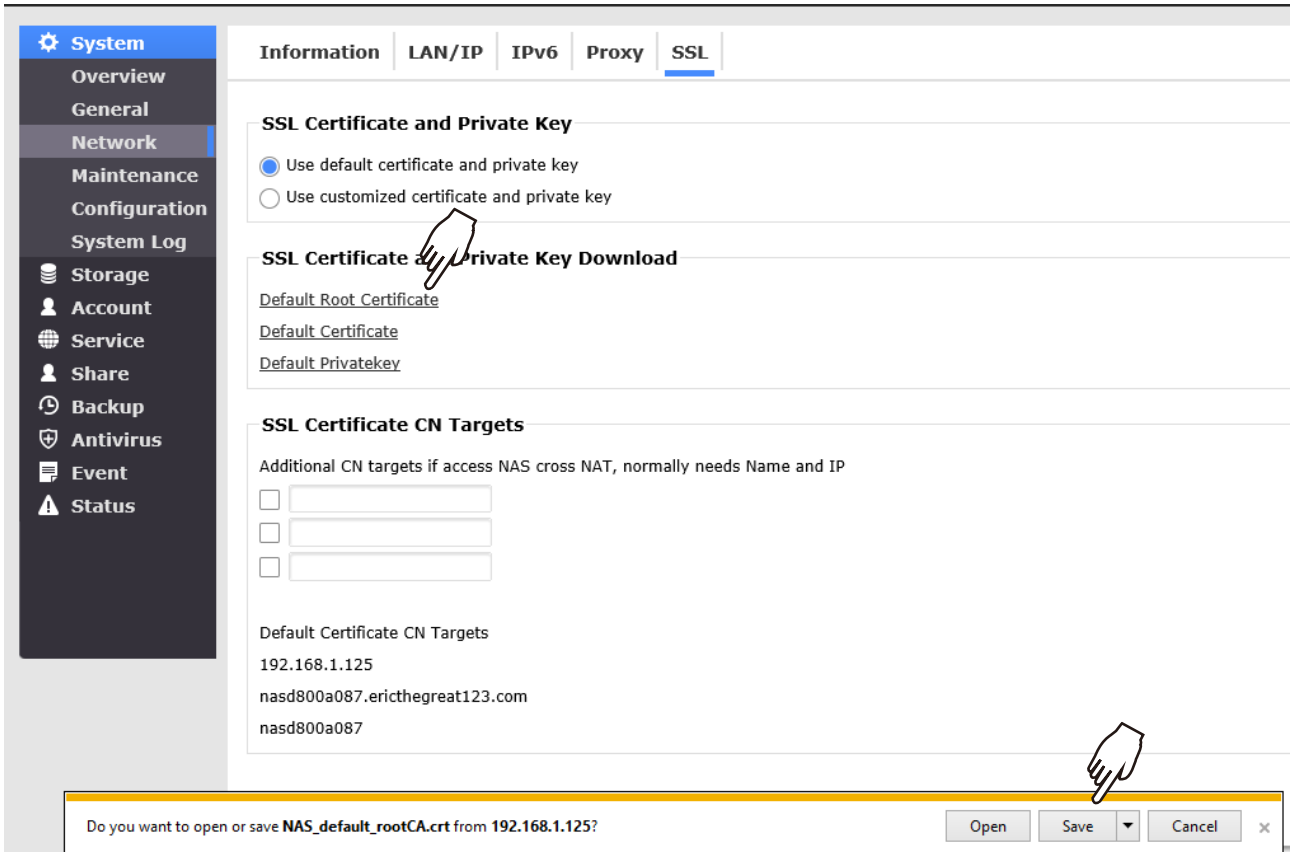


The NAS server enables secure web access by supporting SSL 3.0, both for the user homepage and the administration homepage. To use SSL 3.0, the NAS server will generate a server certificate for authentication and data encryption. By default, the server certificate is issued to the NAS server designated by its IP address. You can also specify to use the server's full name on the server certificate.

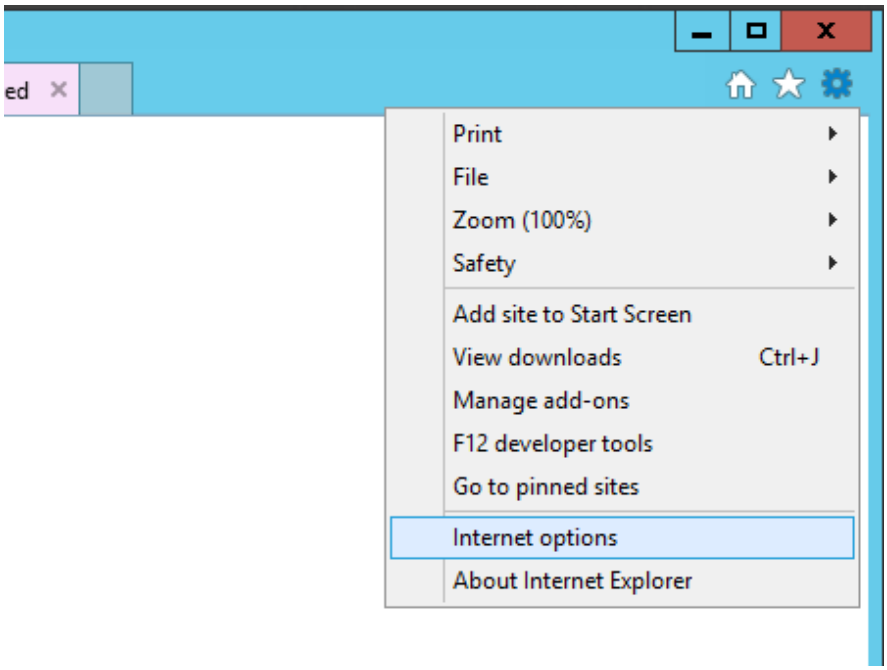
For clients to access server web-pages with secure connection, they have to install the CA certificate first. First go to the **Network→SSL** page. Click Download and install CA certificate hyperlink. Choose to install the certificate when a dialog-box pops up. Once the CA certificate is installed, the client can access all NAS server's web pages via SSL encrypted connection. Suppose that the server IP address is 192.168.1.10. To access the NAS system's web pages with SSL connection, please open https://192.168.1.10/ for the user homepage, or https://192.168.1.10/admin/ for the administration homepage. If the server certificate with the server name is chosen, please open https://[server_name] instead.

To utilize encrypted access, follow the steps below:

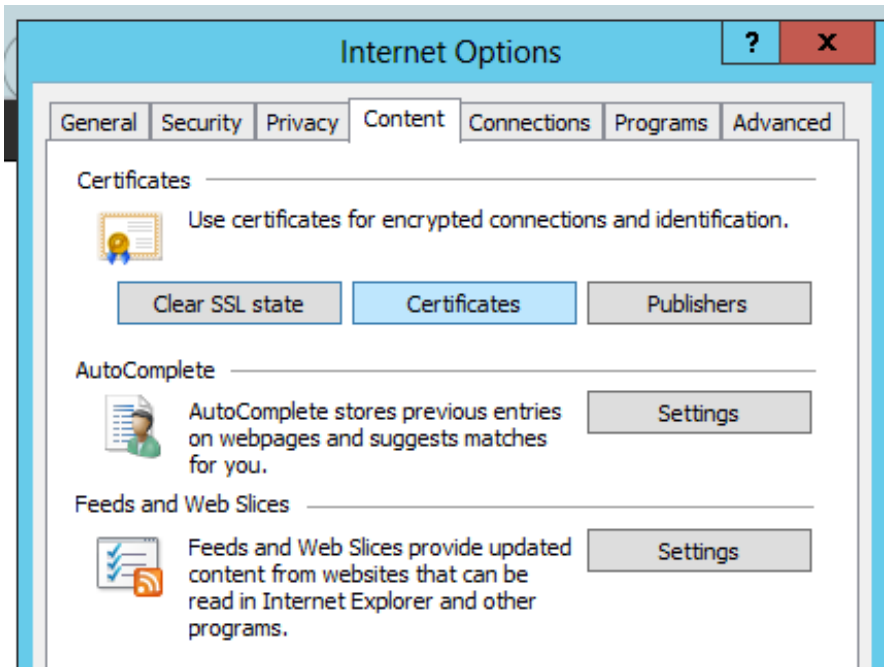
1. On the System > Network page, click on **Default Root Certificate** to download the CA. Save the certificate to preferred location.



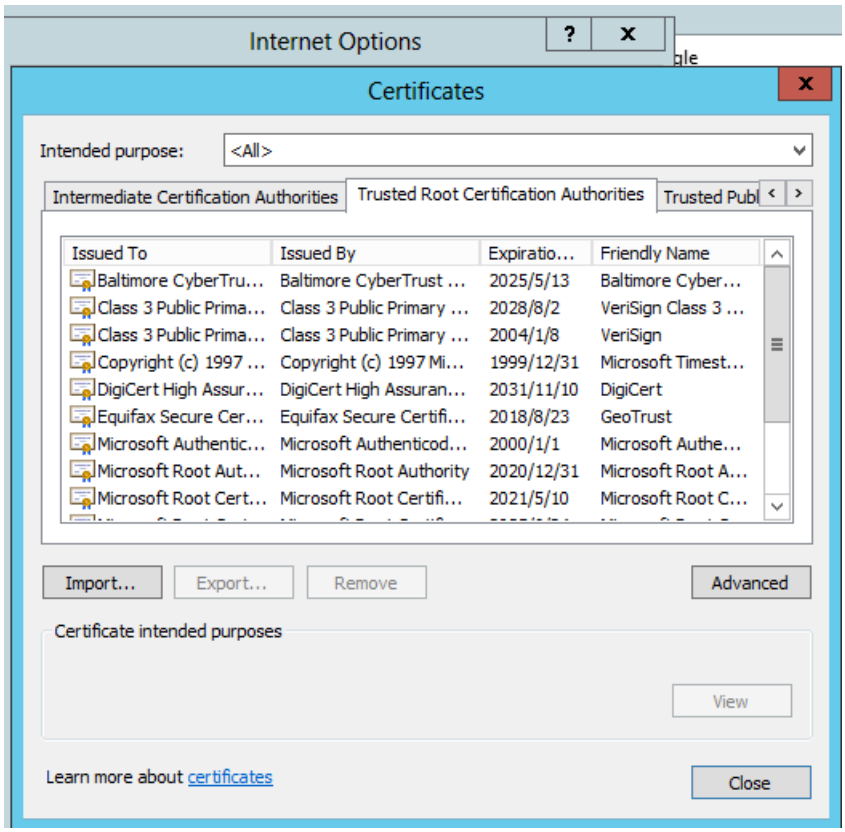
2. On the management computer, open a web browser, e.g., IE. Click on the Tools button, and enter the **Internet options** page.



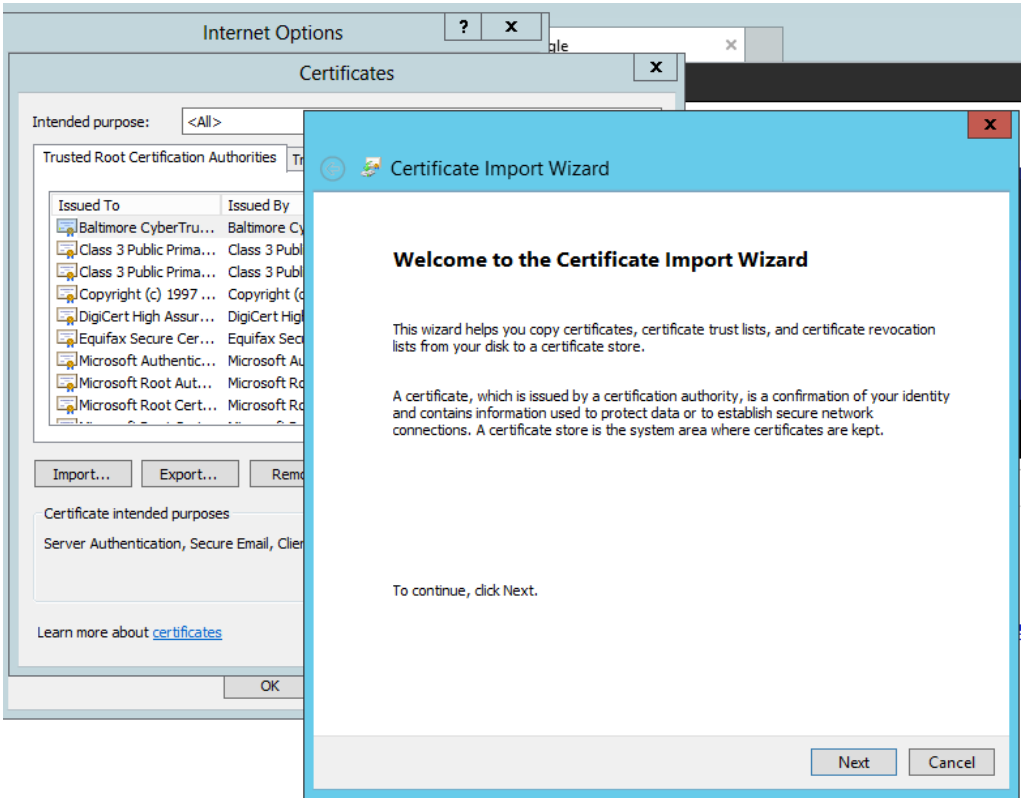
3. Click **Content**, and **Certificates** on the Internet Options page.



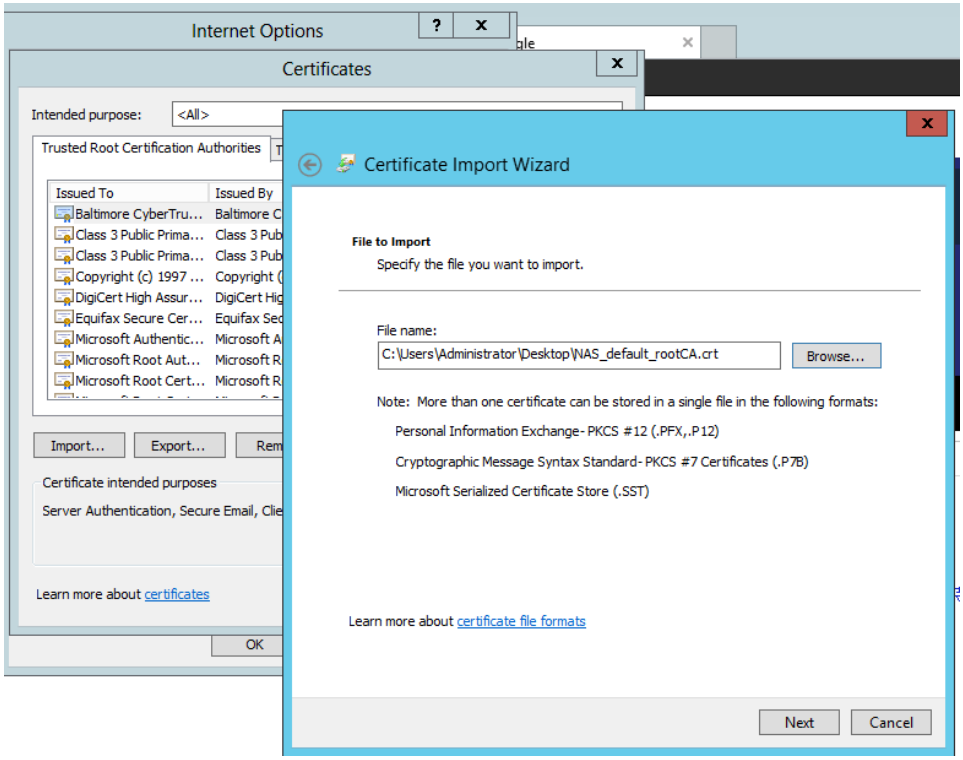
4. Click to open the **Trusted Root Certification Authorities** tab. Click the **Import** button.



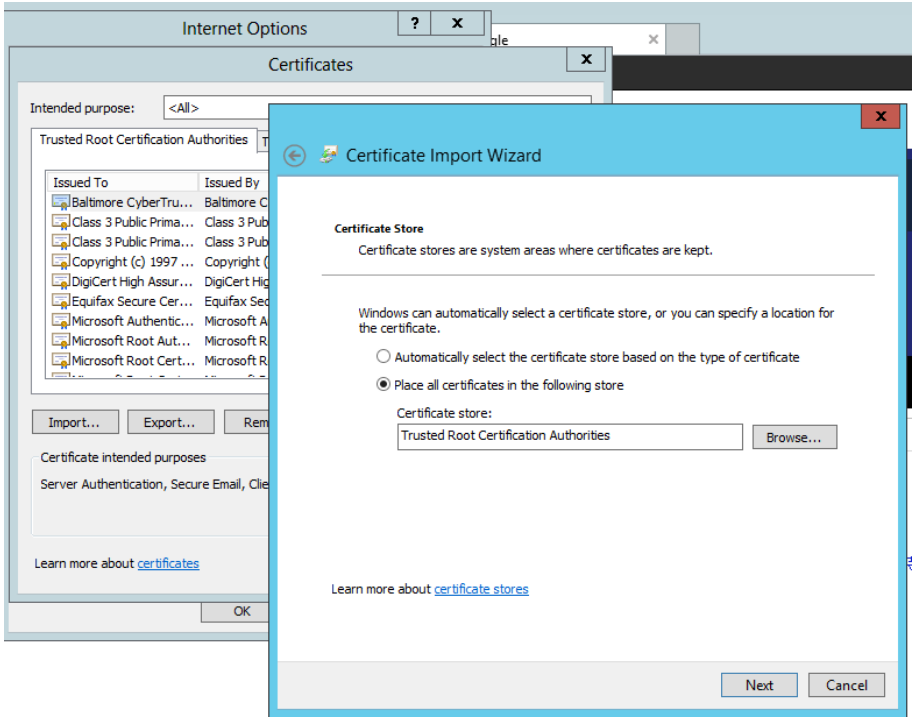
5. The **Import Wizard** page will start. Click **Next**.


Internet Options
Certificates
Intended purpose:
<All>
Trusted Root Certification Authorities
Issued To
Issued By
Import...
Export...
Certificate intended purposes
Server Authentication, Secure Email, Clie
Learn more about certificates
OK
Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
Next
Cancel

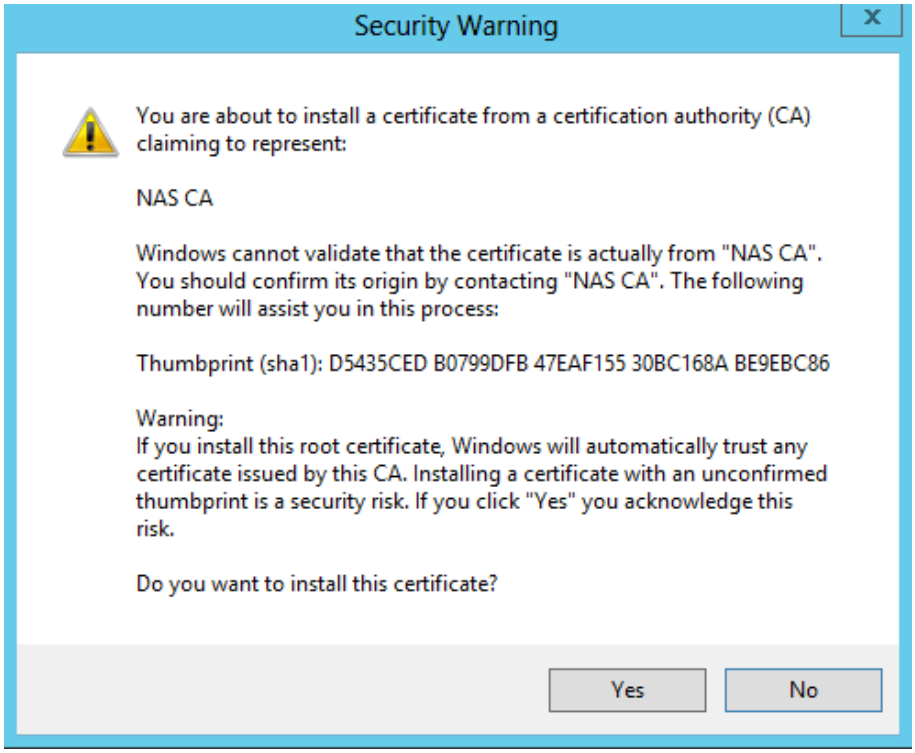
6. Click **Browse** to locate the certificate file you download. Click **Next** to proceed.



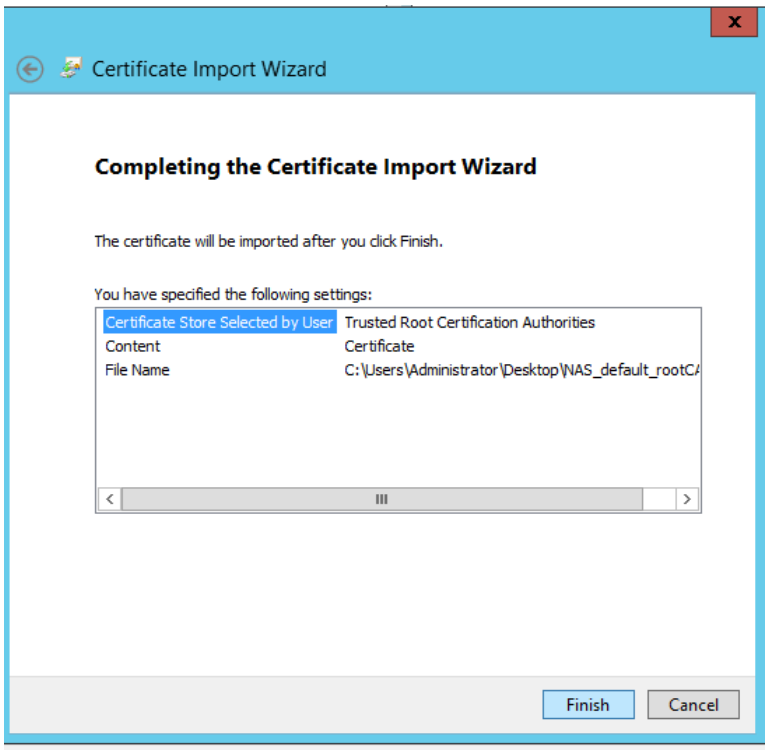
7. Select the location where you want to store the certificate and related information.



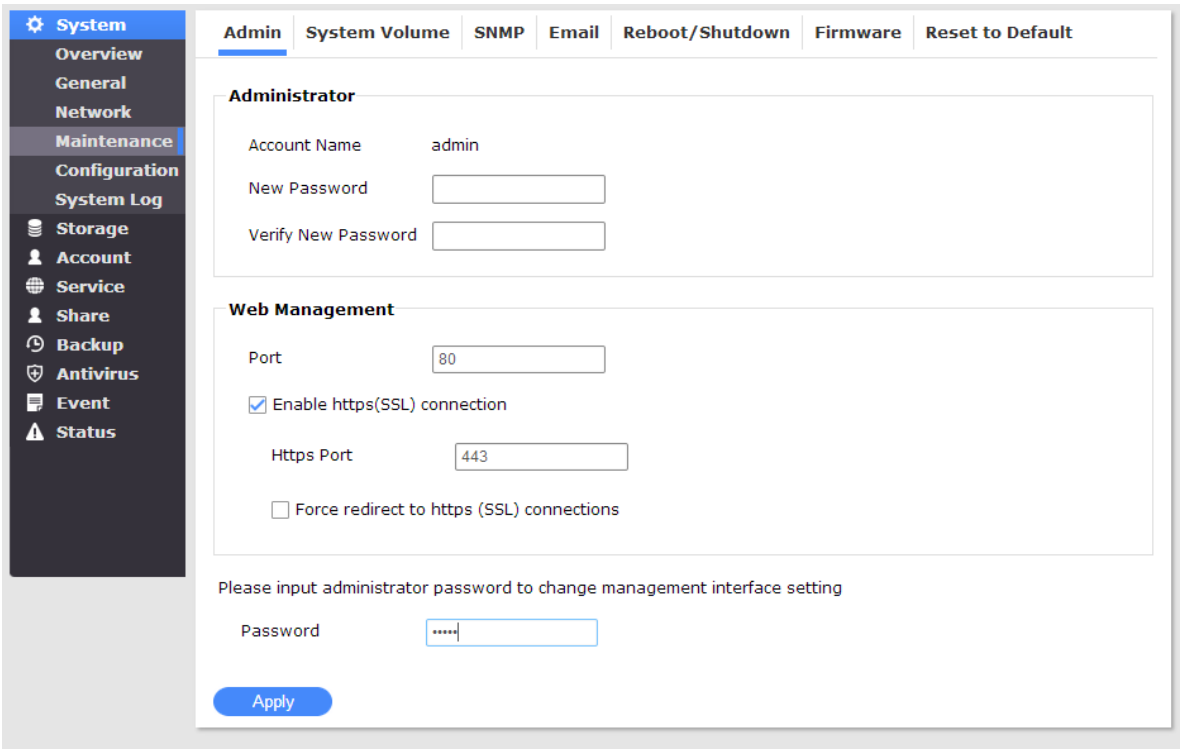
8. Click **Yes** on the Security Warning prompt.


Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
NAS CA
Windows cannot validate that the certificate is actually from "NAS CA". You should confirm its origin by contacting "NAS CA". The following number will assist you in this process:
Thumbprint (sha1): D5435CED B0799DFB 47EAF155 30BC168A BE9EBC86
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No

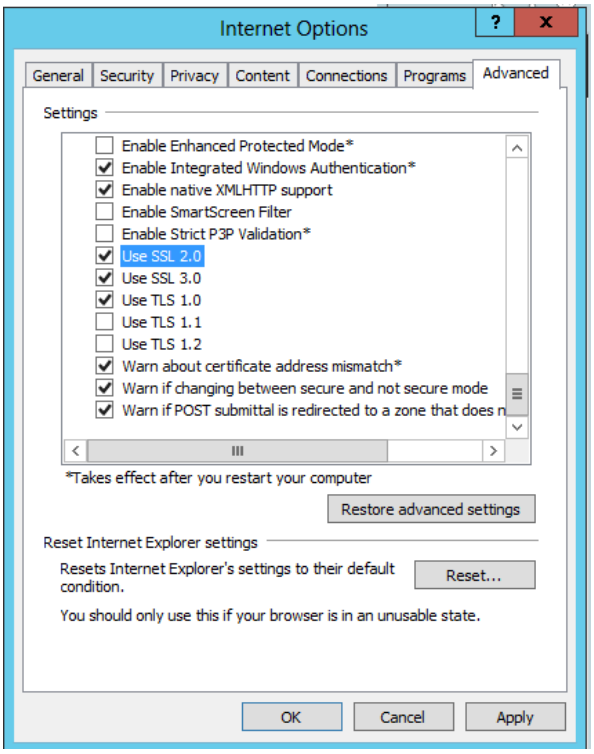
9. Click **Finish** to complete the process.



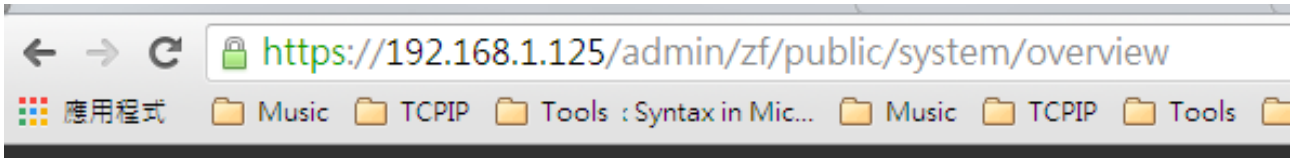
10. Now return to the NAS sever console, **System** > **Maintenance**. Select the **Enable https(SSL) connection** checkbox and enter the default **Https Port number** (default is 443). On leaving the page, enter the administrator's login password, and click the **Apply** button.



11. Also make sure the **SSL** option has been enabled on your browser's Internet Options.

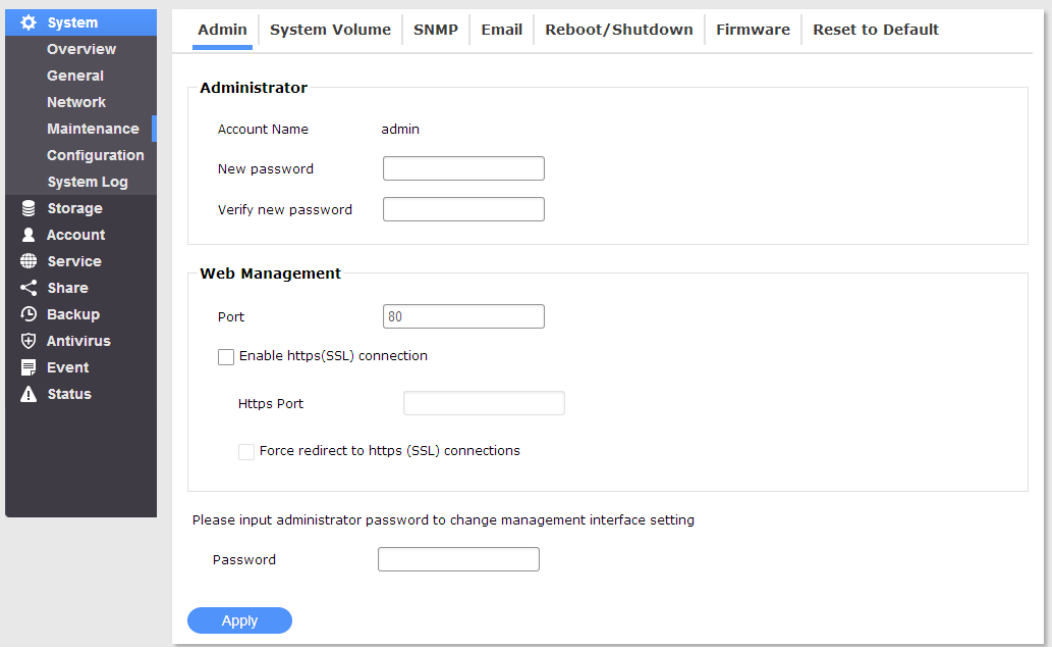


12. You can now enter <https://NAS server IP address/> to start a secure and encrypted management access.



3.5. System > Maintenance

The Maintenace page provides access to Administrator's account, System Volume, SNMP, Email, Reboot/Shutdown, Firmware-related, and reset to default settings.



3.5.1 System > Maintenance > Admin

This window provides you with the configuration options to change the Administrator's password. The default Account Name is admin, and this can not be changed. It is highly recommended to provide a secure password with the combination of alphabetic, symbol, and numeric characters as the administrator's password.

Web Management - The default management access is via TCP port 80. You can assign a different HTTPS port for access through the Internet, and through a firewall. If a different https port has been assigned and opened on the router, specify its TCP port so that management access is made through that port.

Finally, if the above changes were made, make sure you enter the system administrator's password before your click on the **Apply** button.

3.5.2 System > Maintenance > System Volume

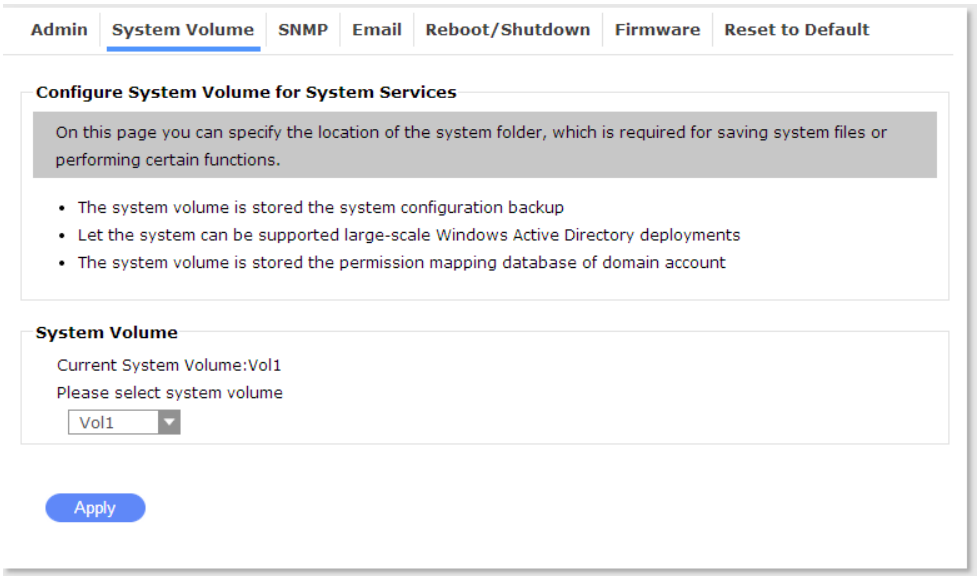
Configure System Volume for System Services

You can specify the location of the system Folder Group, which is required for saving system files or performing related functions.

System Volume

If you have created more than one volume, you can specify which is the default system volume. This option will only appear after you configured a storage volume.

The information on this page is mainly for the user reference.

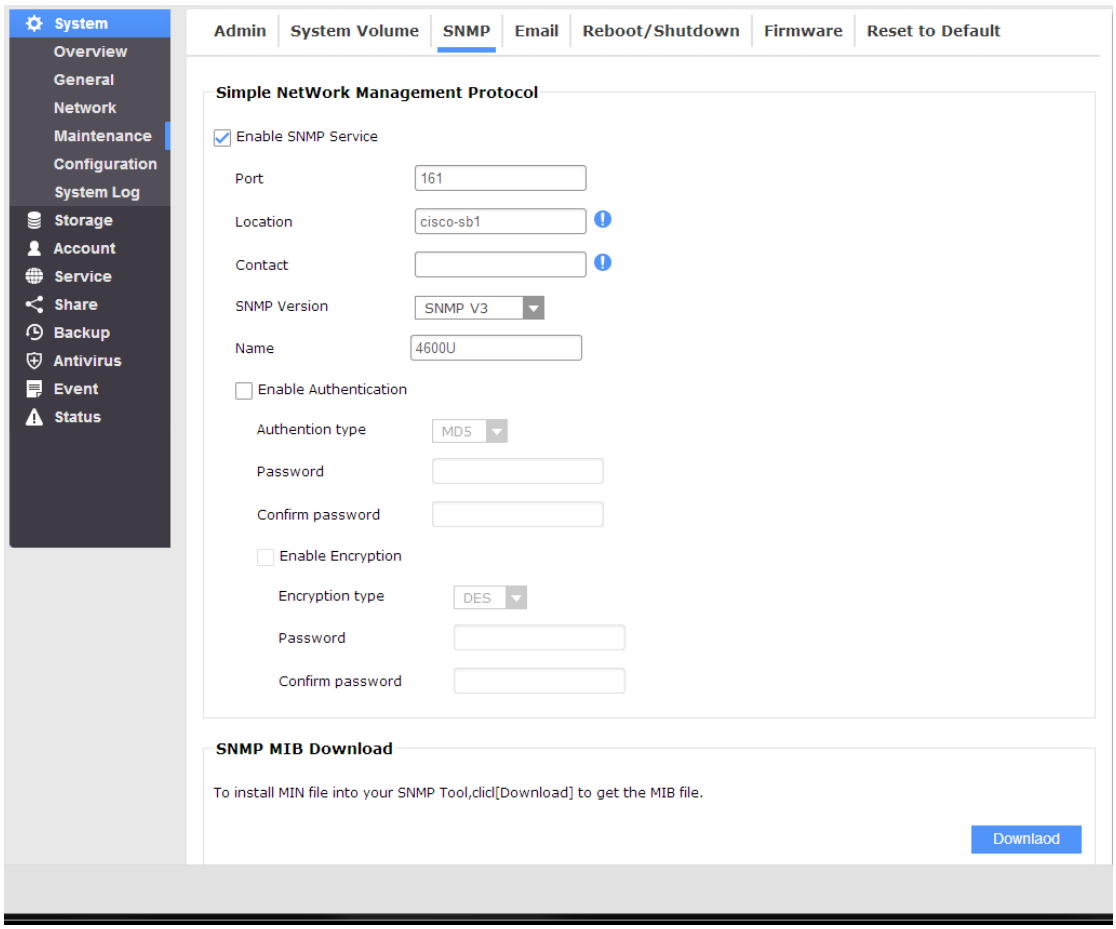

Admin
System Volume
SNMP
Email
Reboot/Shutdown
Firmware
Reset to Default
Configure System Volume for System Services
On this page you can specify the location of the system folder, which is required for saving system files or performing certain functions.
The system volume is stored the system configuration backup
Let the system can be supported large-scale Windows Active Directory deployments
The system volume is stored the permission mapping database of domain account
System Volume
Current System Volume:Vol1
Please select system volume
Vol1
Apply

3.5.3 System > Maintenance > SNMP

Simple network management protocol (SNMP) allows system administrators to access NAS server operating statuses via a 3rd-party SNMP software. The SNMP trap related configuration is found in the **Event** > **Configuration** window. If only SNMP trap service is preferred, you may not need to enable the service in here.

To utilize the SNMP service,

1. First enable the SNMP service, community name, select SNMP version, and download the **MIB** file.



Community: A name serves as a simple authentication. The communication between the SNMP management console and the NAS server cannot be established if the community names do not match.

Port: Default is 161, change it if necessary.

Location: Provide location information of the SNMP agent.

Contact: Provide name of the contact person who has the management information of the SNMP agent.

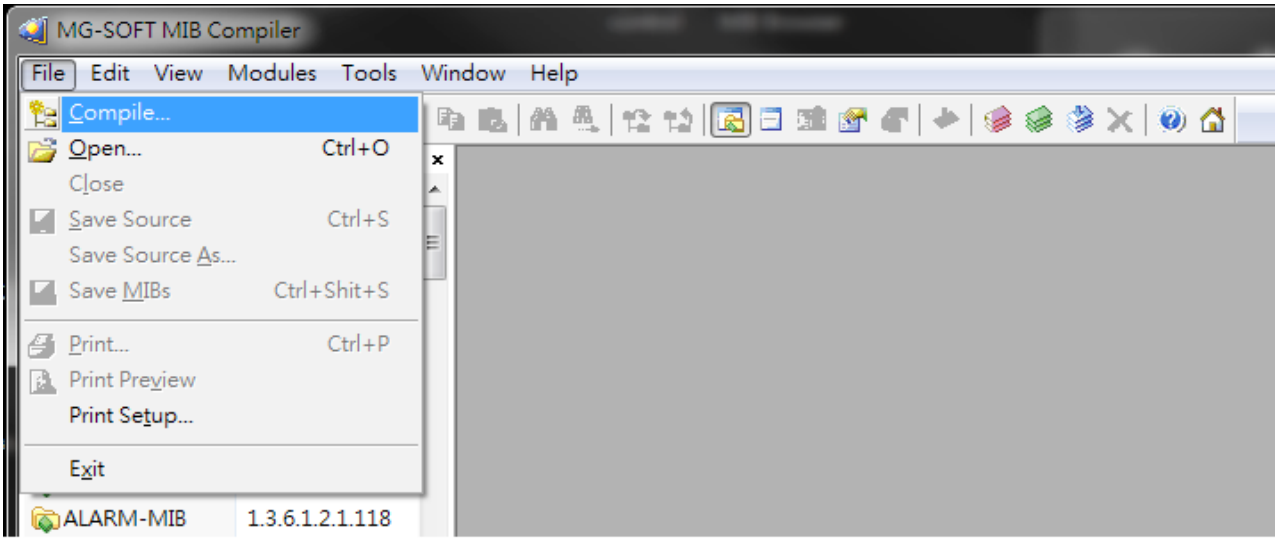
SNMP Version: Specify the supported SNMP service revision that is identical on your management software and the NAS server.

Community: If the SNMP service is enabled within a community configured within your LAN, specify the name of the community.

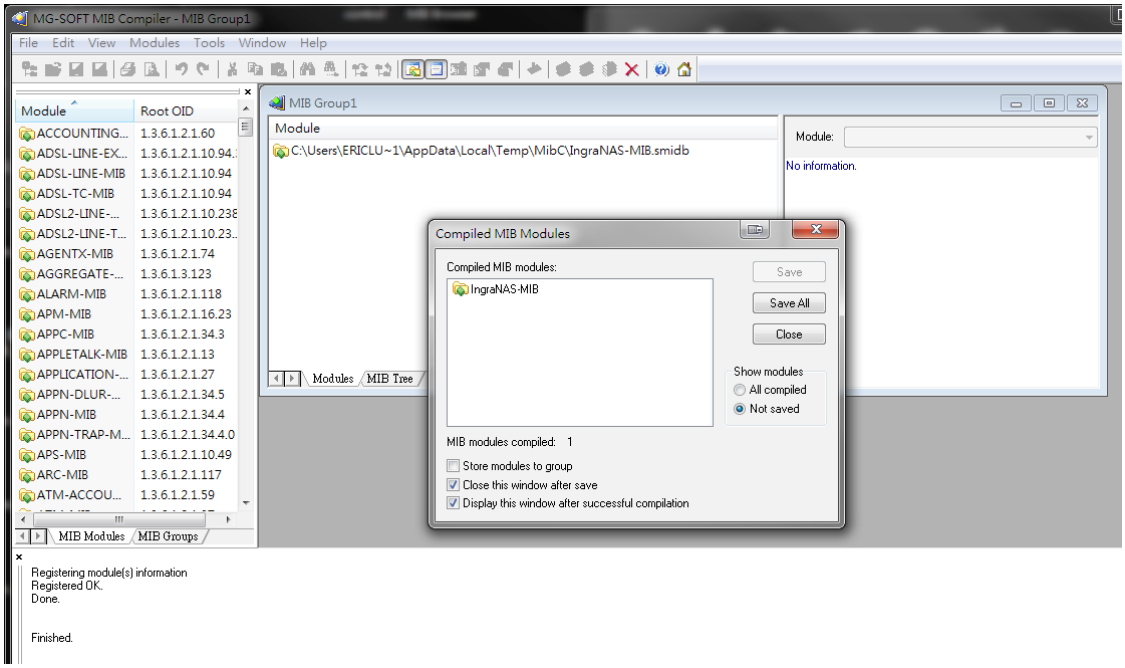
2. Please download or acquire MG-SOFT MIB browser (or similar SNMP utility):

http://www.mg-soft.si/download.html

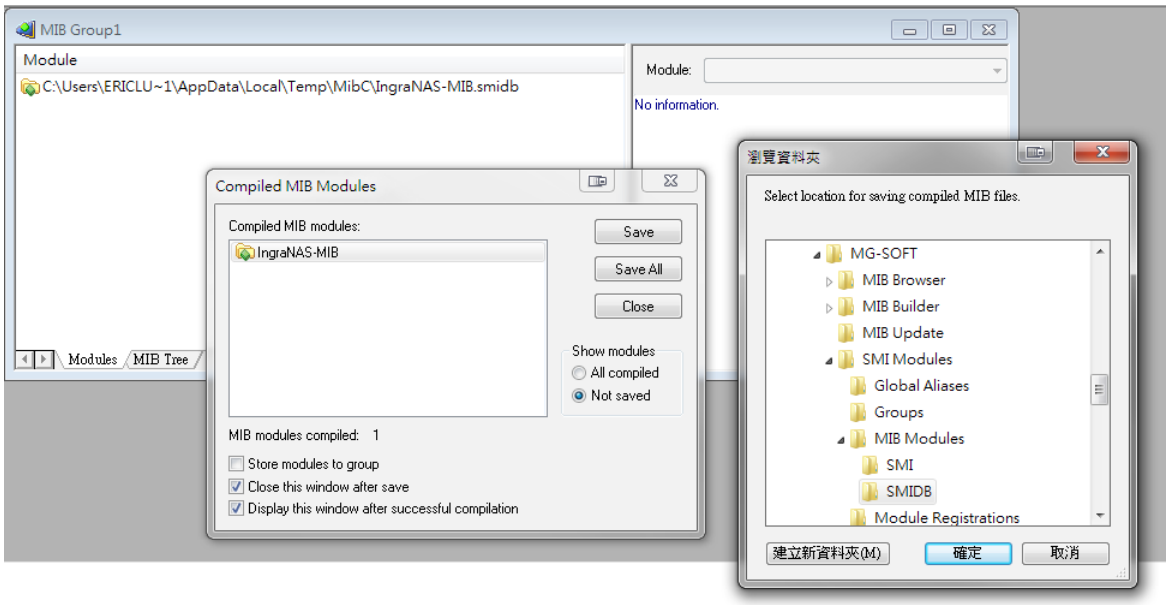
3. Open the **MG-SOFT MIB Compiler**, and select the NAS server's MIB file you previously downloaded. .

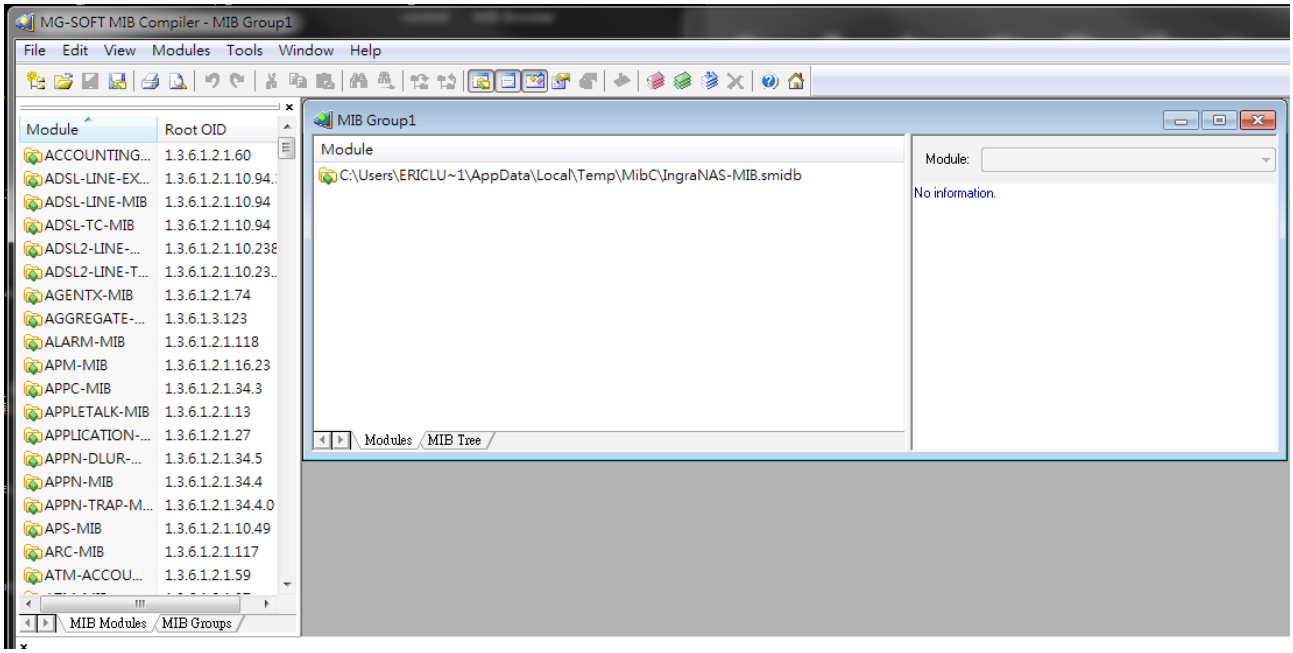


4. Select the Ingrasys MIB module and then click **Save** to proceed.

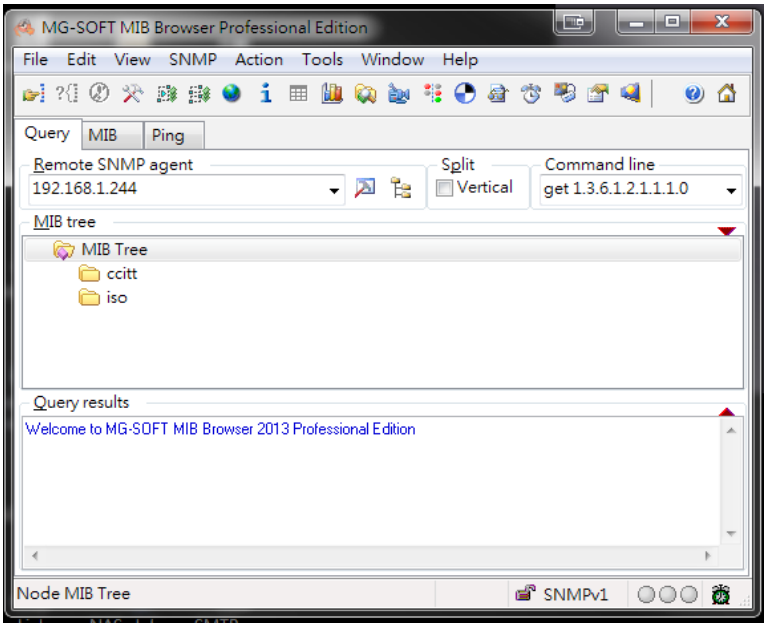


5. Save the compiled module to a position as shown below.

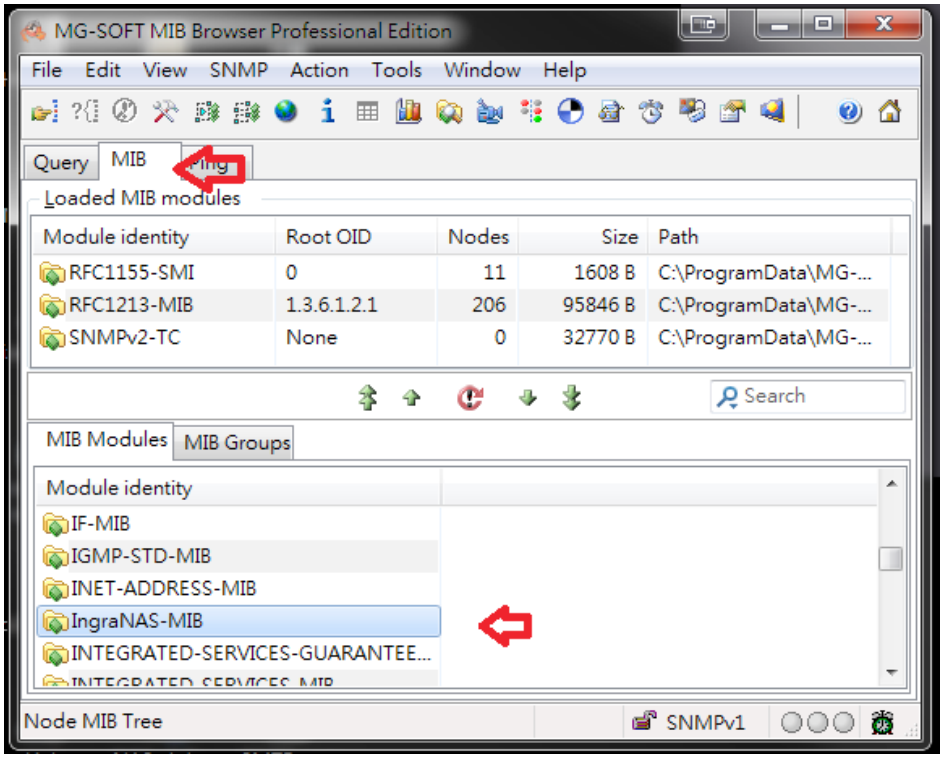




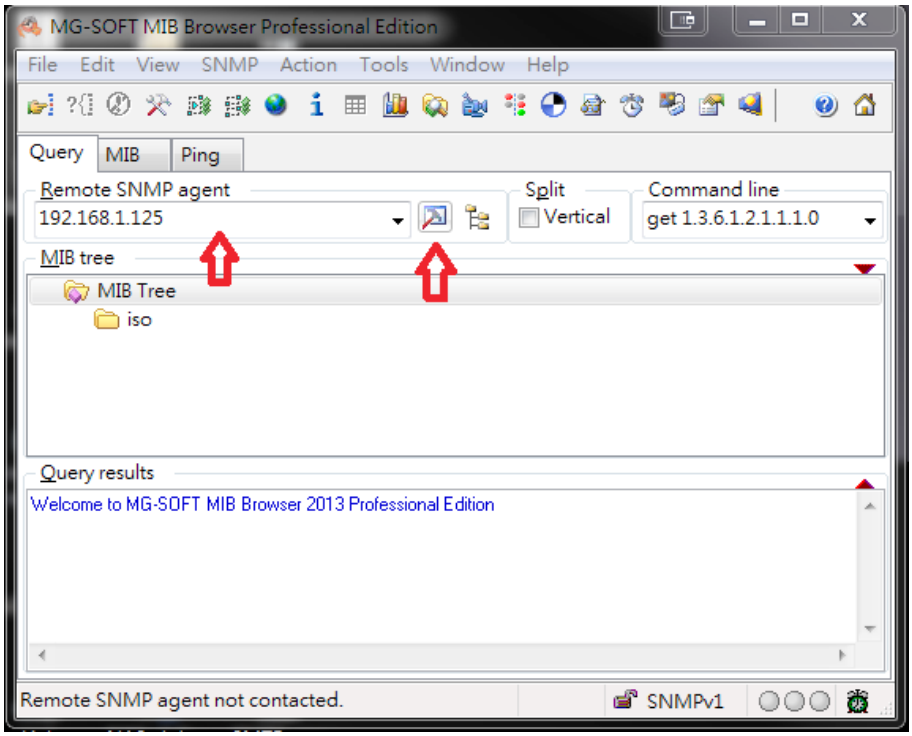
6. Open the MIB browser.



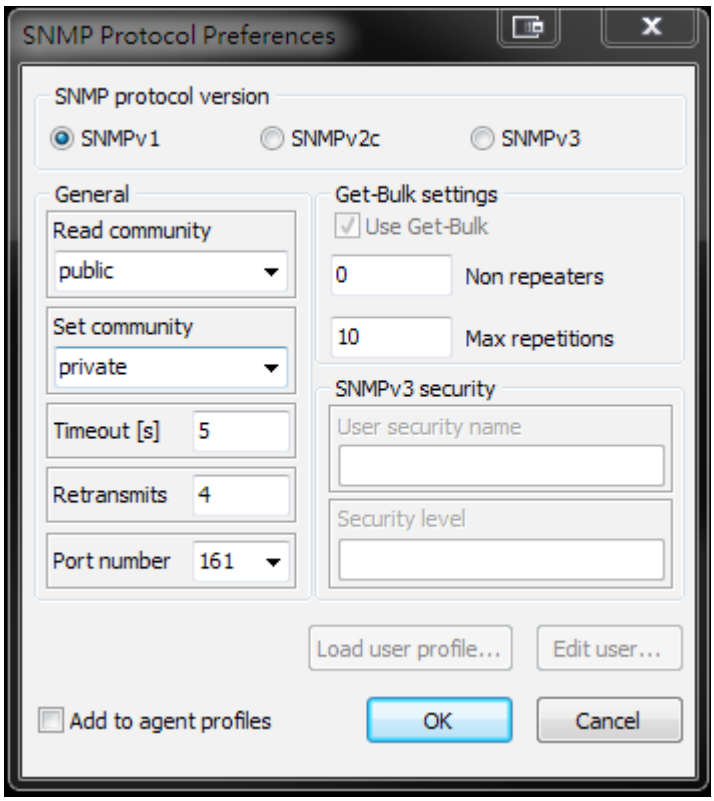
7. When the MIB browser is started, click on the **MIB** tab. Search and locate the IngraNAS-MIB module from the list below.



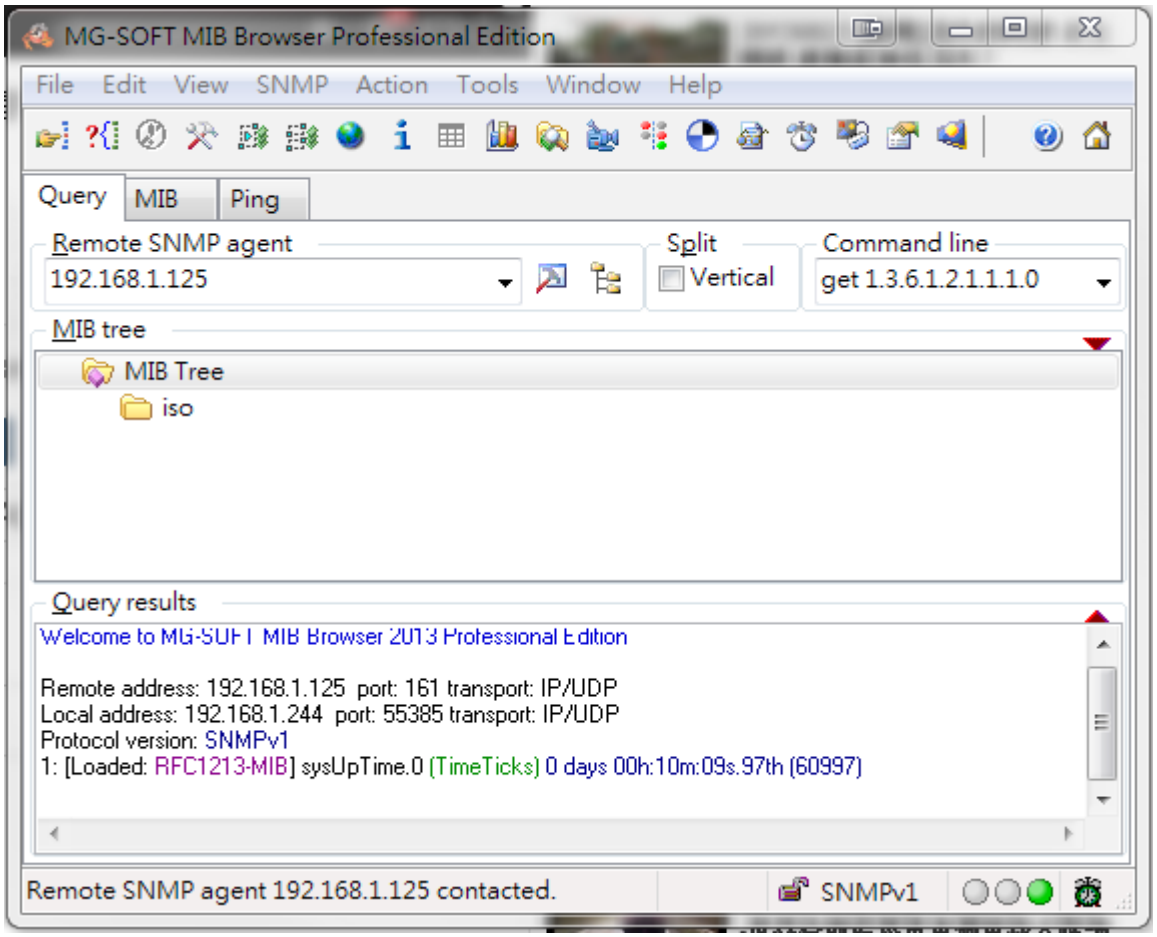
8. Enter the Remote **SNMP agent's IP** (that of your NAS server), and then click on the **Query** button.



9. The **SNMP Protocol Preferences** window will prompt. Configure the SNMP version, Community settings to the same configuration on your NAS server.



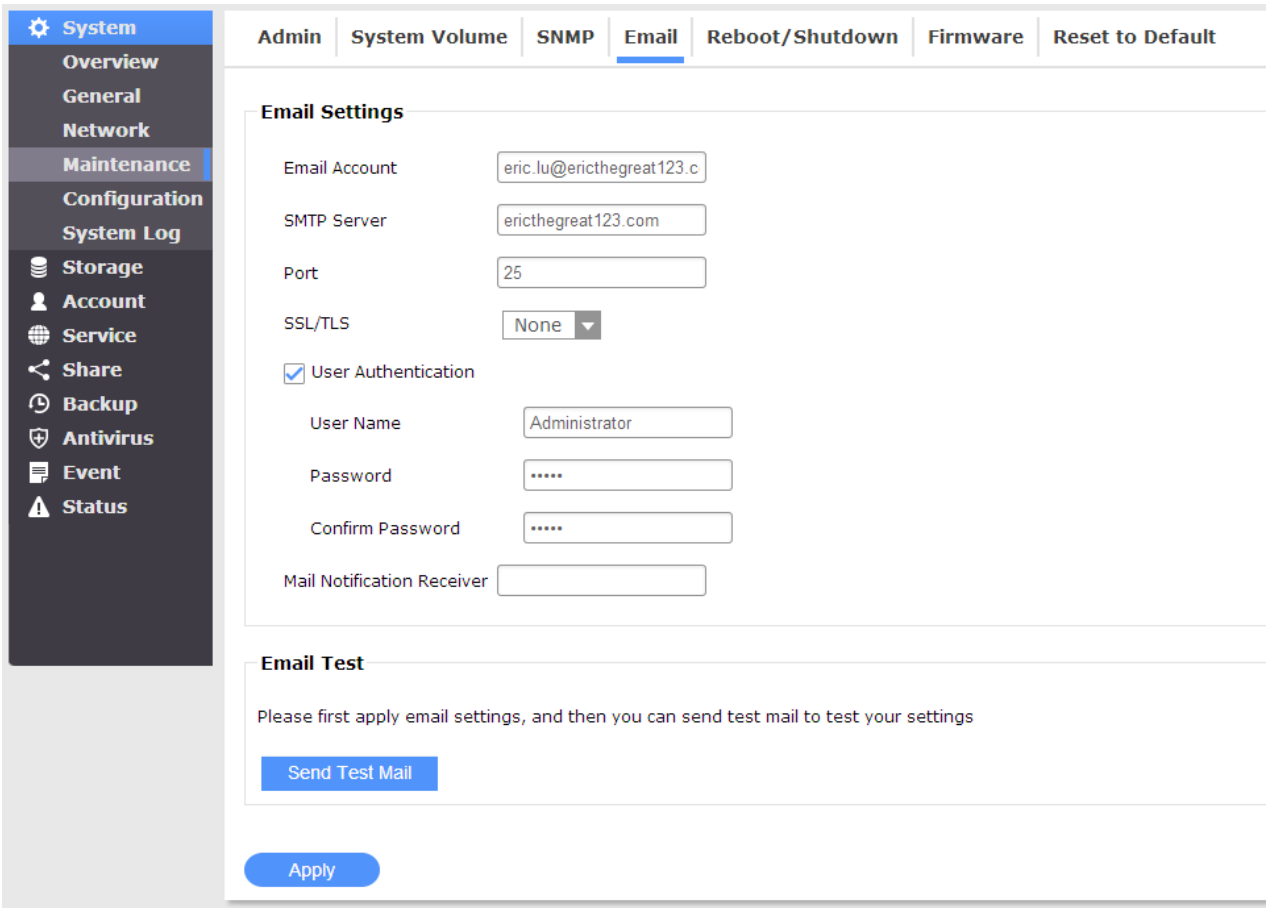
10. When successfully connected, the Ingrasys MIB location will be shown. Note that currently the NAS server supports the **Get** command only. Right-click on the MIB profile entry to select the Get command.



3.5.4 System > Maintenance > Email

To enable Email notification from the server,

1. Enter a valid email account, an SMTP server address, and if SSL certification is required, select the SSL option. Note that TLS certification is currently not supported.
2. Next, enter the User Name, Password, and the address of a Mail Notification Receiver.
3. Click on the Apply button.
4. Click on the Send Test Mail button to see if you can receive a test Email from the receiver's mail address.



3.5.5 System > Maintenance > Reboot/Shutdown

Shutdown and **Reboot**

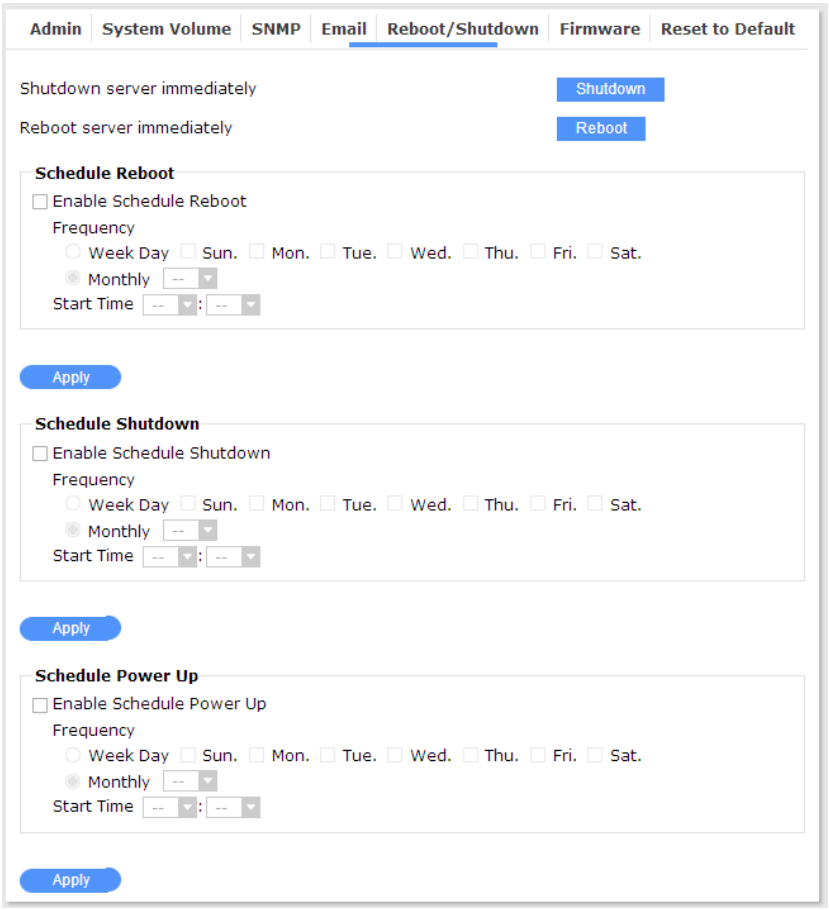
In addition to the quick access button on the upper-right of the management session, you can reboot or shutdown the server from here.

Schedule Reboot

You can configure the server to reboot according to a preset schedule.

1. Select the checkbox to enable the schedule. The options and pull-down menus will then be enabled.
2. Select the day in a week or a day in a month for the reboot to take place.
3. Select a **Start Time**, and click on the **Apply** button.

You can also configure a scheduled Shutdown using the method described above.



You can configure the server to automatically power up by a preset schedule.

1. Select the checkbox to enable the schedule. The options and pull-down menus will then be enabled.
2. Select the day in a week or a day in a month for the power-on to take place.
3. Select a **Start Time**, and click on the **Apply** button.

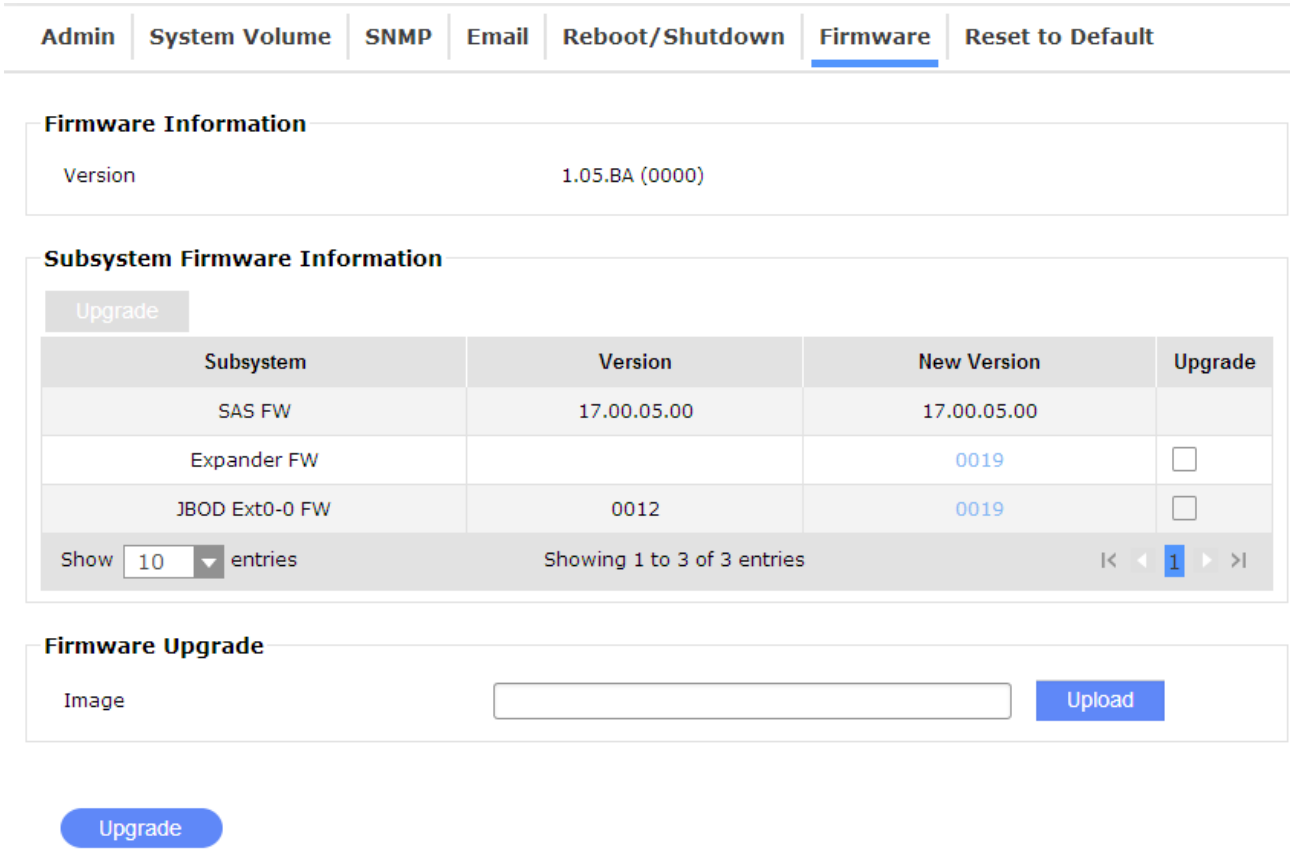
3.5.6 System > Maintenance > Firmware

This window provides information about the current firmware revision, and the option to upgrade the current firmware.

To upload a firmware, first you should download the firmware from Ingrasys' website: www.Ingrasys.com. Save the firmware file to your management PC. Use the **Upload** button to locate the firmware file, and then click the **Upgrade** button to proceed.

NOTE:

1. Your current file services will be interrupted, because the upgrade process will reboot your server.
2. When upgrading firmware, please visit the Status > Task Progress window to check if any application is still running. If so, please wait for the application to complete, or manually end the progress to ensure that a running application is not inappropriately ended.

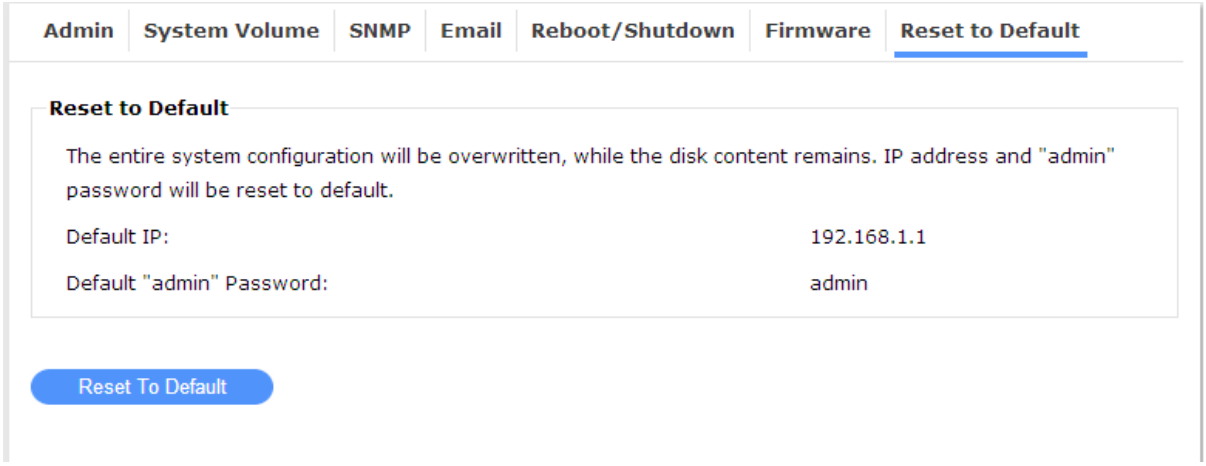


You can also click to select to upgrade the SAS expander, SAS, and JBOD chipsets firmware.

3.5.7 System > Maintenance > Reset to Default

This window allows you to restore system defaults. All previous system configuration will be erased and returned to factory defaults. The data stored on your disk volume will remain intact.

Note that the server IP will be restored to 192.168.1.1, and the default password will become the original "admin".



3.6. System > Configuration

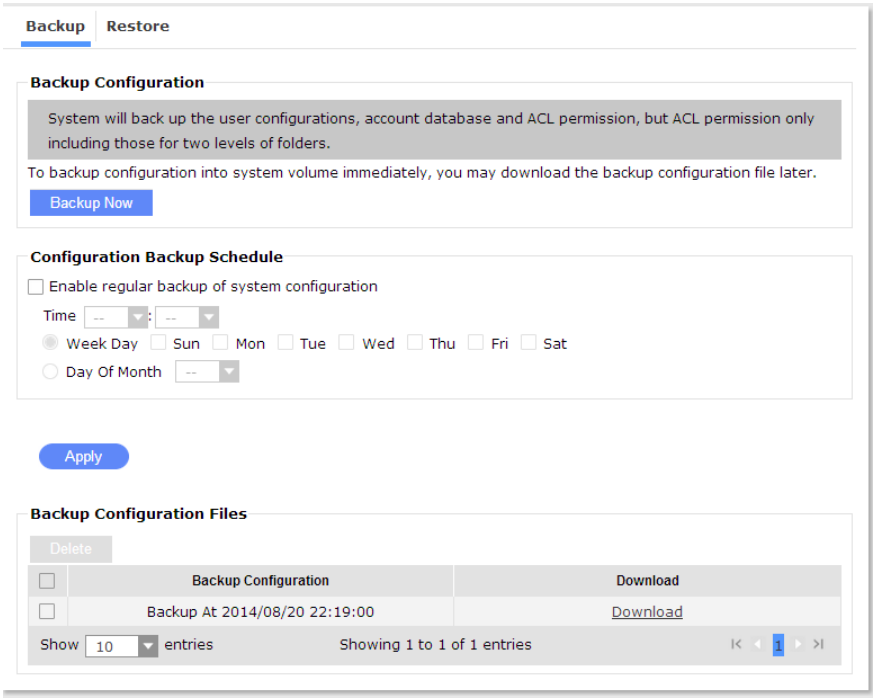
The Configuration page provides means to back up your system configuration.

1. **Backup Configuration**: Immediately creates a backup of your current configurations.
2. **Configuration Backup Schedule**: Click the checkbox to enable the options and pull-down menus. You can then specify a day for the backup to take place on a daily or monthly basis. Click the **Apply** button for the configuration to take effect.

The system configuration backup will be saved to a preserved space on your storage volume. A list of previous backups will be automatically displayed at the bottom. You can click the **Download** button to save the backups to your PC.

If you should need the help of our technical support, you can also download and send the configuration file to our engineers.

To delete a backup, click the checkbox in front and then click the **Delete** button.

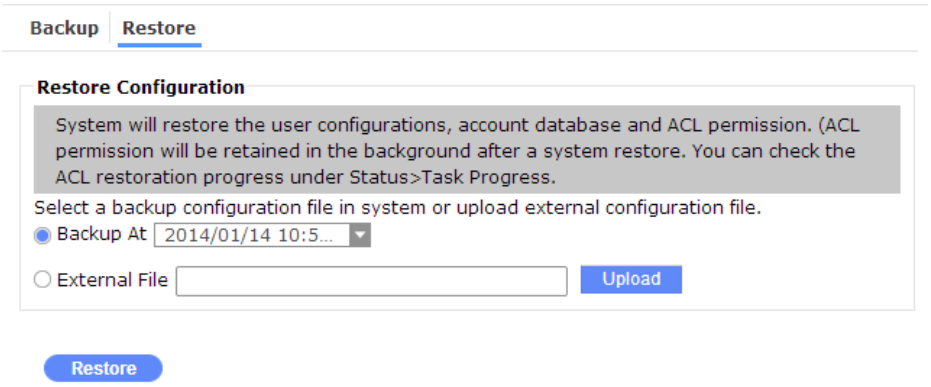


NOTE:

1. The system will automatically back up the user configuration, including account database and ACL permissions. However, the ACL permission thus backed up will include the information for two directory levels down.
2. We highly recommend backing up a copy of system configuration to your management computer. If the need should arise for maintenance, you will have a system configuration backup to restore the NAS server to normal operation in a short time.

The Restore page allows you to restore your current configuration to the previous state using a previous backup.

1. You can select a previous backup using the drop-down menu by selecting the date it was created.
2. If you saved your backup to somewhere else, e.g., a PC that once had a management session, you can upload the backup using the **External File** option.
3. You can then click on the **Restore** button. A server reboot is automatically applied.


Backup
Restore
Restore Configuration
System will restore the user configurations, account database and ACL permission. (ACL permission will be retained in the background after a system restore. You can check the ACL restoration progress under Status>Task Progress.
Select a backup configuration file in system or upload external configuration file.
Backup At
2014/01/14 10:5...
External File
Upload
Restore

3.7. System > System Log

The System Log page provides access to the configuration of event logs.

1. **Log Level**: You can specify what types of event logs to be delivered and preserved. If you select 0 (Emergency), then only the most critical events will be reported.
   If you select 6 (Informational), then notifications of all severity levels will be reported. The smaller the number, the fewer the instances of event messages.

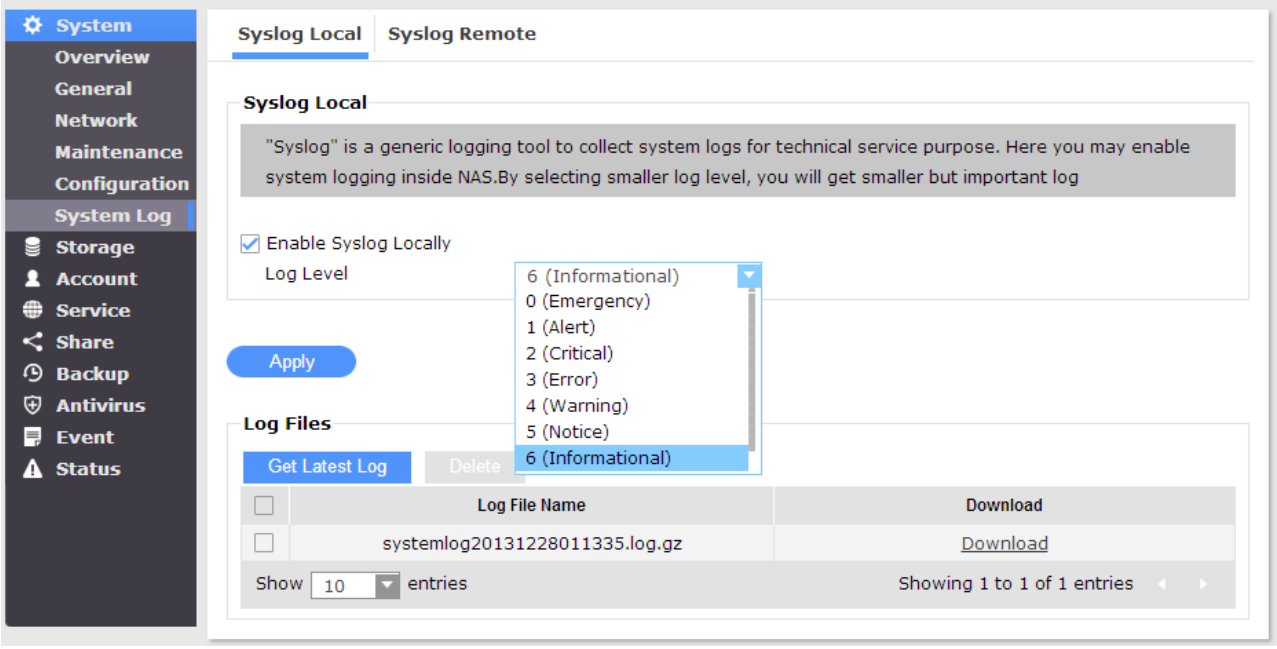
   When done, click on the **Apply** button.

2. **Get Latest Log**: Click the Get Latest Log button to retrieve a system log record. You can then download the system log to your PC.

The system log file will be saved to a preserved space on your storage volume. A list of previous logs will be automatically displayed at the bottom. You can click the **Download** button to save the backups to your PC.

If you should need the help of our technical support, you can also download and send the event log file to our engineers.

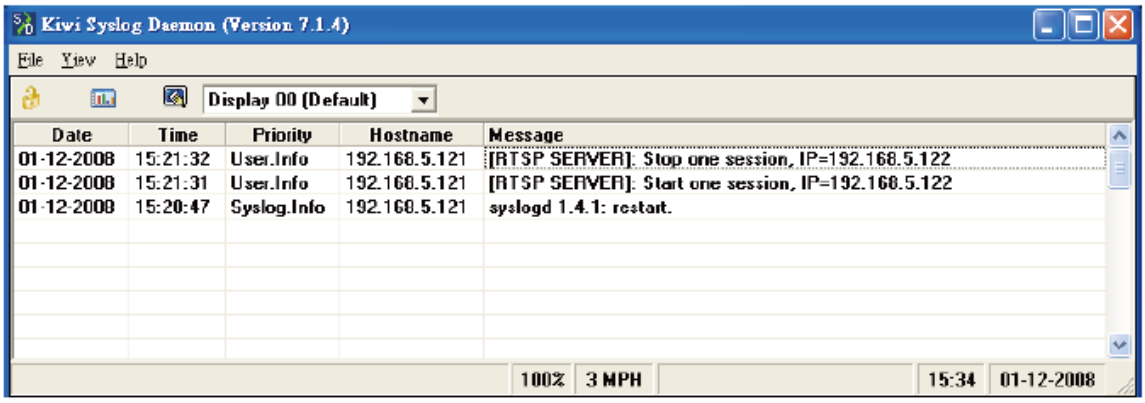
To delete a Log file, click the checkbox in front and then click the **Delete** button.



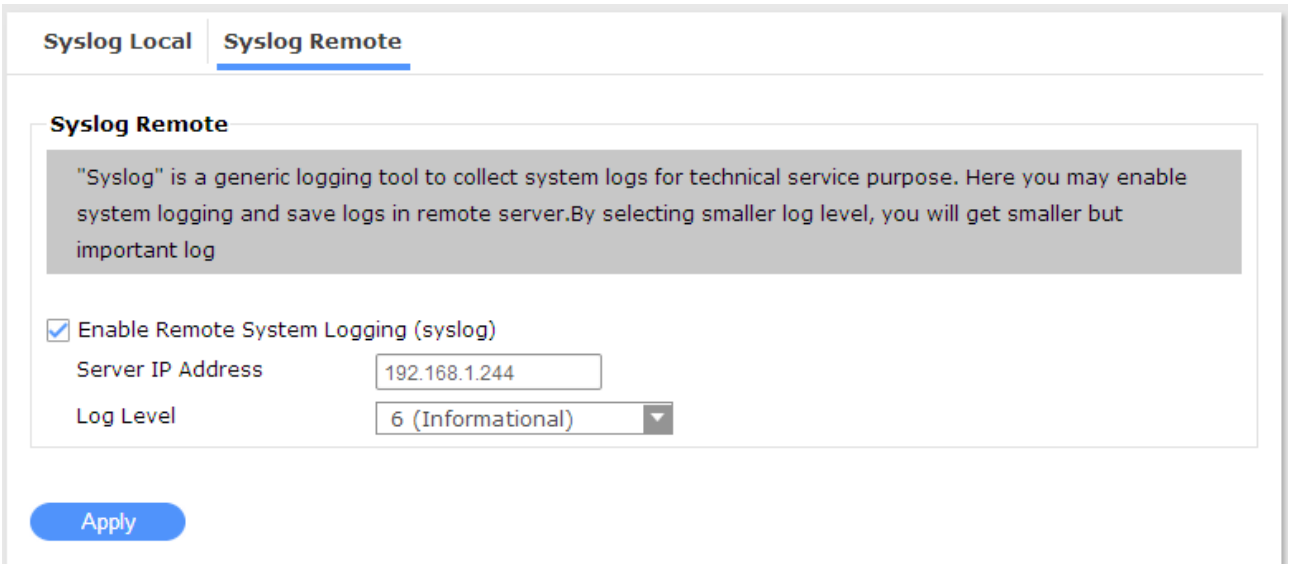
To view a downloaded log file, please use the UltraEdit or PSPad to open the log files.

3.7.1 System > System Log > Syslog Remote

You can configure the server to send system logs to a remote server as a log backup. Before using this feature, it is suggested that you install a log-recording tool such as the Kiwi Syslog Daemon from http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/.


Kiwi Syslog Daemon (Version 7.1.4)
File View Help
Display 00 (Default)
Date Time Priority Hostname Message
01-12-2008 15:21:32 User.Info 192.168.5.121 [RTSP SERVER]: Stop one session, IP=192.168.5.122
01-12-2008 15:21:31 User.Info 192.168.5.121 [RTSP SERVER]: Start one session, IP=192.168.5.122
01-12-2008 15:20:47 Syslog.Info 192.168.5.121 syslogd 1.4.1: restart.
100% 3 MPH 15:34 01-12-2008

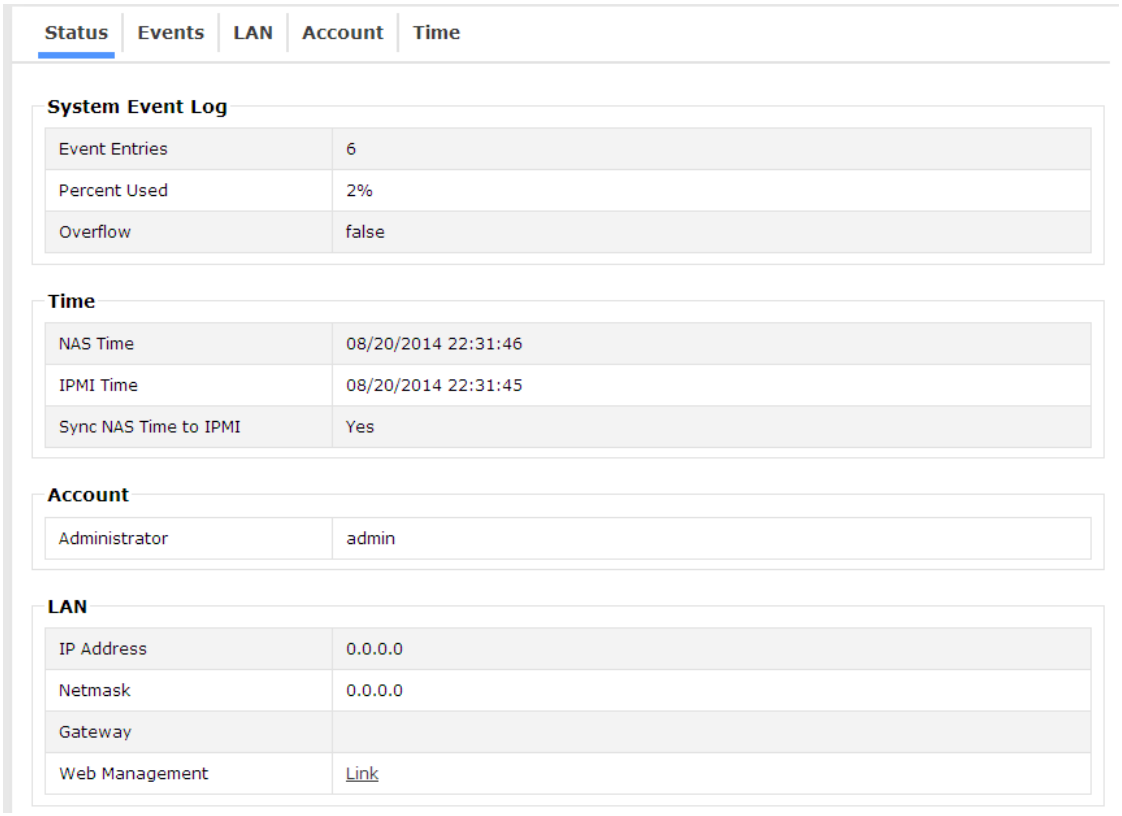
To enable remote log, select the checkbox, enter the IP address where the log-recording software resides, select the log level, and then click on the **Apply** button.


Syslog Local
Syslog Remote
Syslog Remote
"Syslog" is a generic logging tool to collect system logs for technical service purpose. Here you may enable system logging and save logs in remote server.By selecting smaller log level, you will get smaller but important log
Enable Remote System Logging (syslog)
Server IP Address
192.168.1.244
Log Level
6 (Informational)
Apply

3.8. System > Platform IPMI

IPMI stands for Intelligent platform Management Interface. The server has the benefits of self management using a BMC (Baseboard Management Controller) processor, which connects CPU and components on the main board for a better awareness of system operating details, including those for temperature, voltage, fan operation, etc. The IPMI operation has the following benefits:

1. Independent operation via an out-of-band connection which is good for a re-start, and is independent regardless of whether the system is on or off.
2. Ease of expansion - sensor or controllers can be easily added.
3. CPU is connected to BMC, which means that the event log can be easily delivered.



This window provides a glimpse of system operation statuses.

The adjacent **Events**, **LAN**, **Account**, and **Time** tabbed windows provide easy access to the system events, LAN settings, the Account setup, and the IPMI time setting which can be synchronized with that on the NAS server.

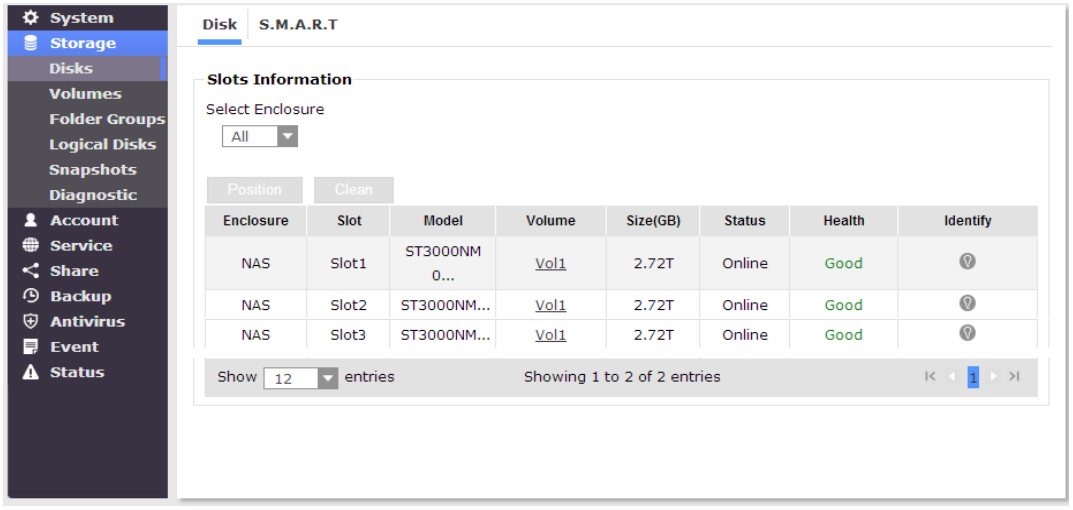
Chapter 4 Storage

The Storage windows provides access to the Disks, Volumes, Folder Groups, Logical Disks, and Snapshot backup configuration options. The concerns about RAID storage composition can be found in **Appendix A** More about RAID Storage on page 156.

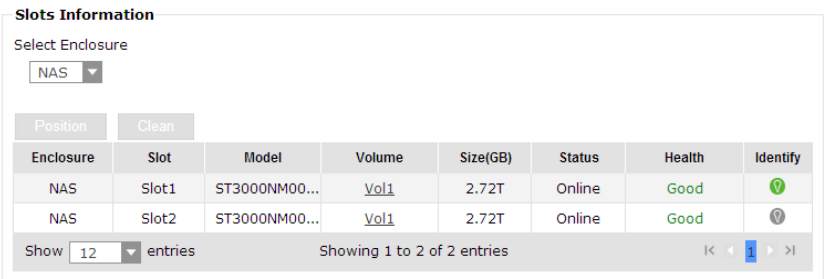
4.1. Storage > Disks

The Storage > Disks page provides access to the current conditions of all disk drives installed in your chassis.

The action button, , lights the disk activity LED of a drive tray for identifying a specific disk drive in a chassis.

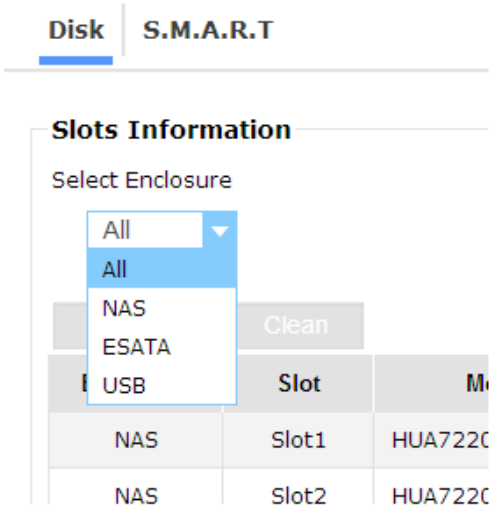


When you need to locate a physical disk drive, click on a disk entry, and then click on the **Position** tab button to display a virtual layout of the position of the currently selected disk drive. Click on the disk drive's **Slot** number to activate the Position button. This is very important if you need to replace a faulty drive.



The LED on the designated drive tray will light Red.

If you have other storage connected to the server, e.g., a JBOD, you can select a different enclosure using the Select Enclosure menu.



S.M.A.R.T.

The second window displays the working status of individual disk drives, including model name, capacity, S.M.A.R.T., state, and temperature.

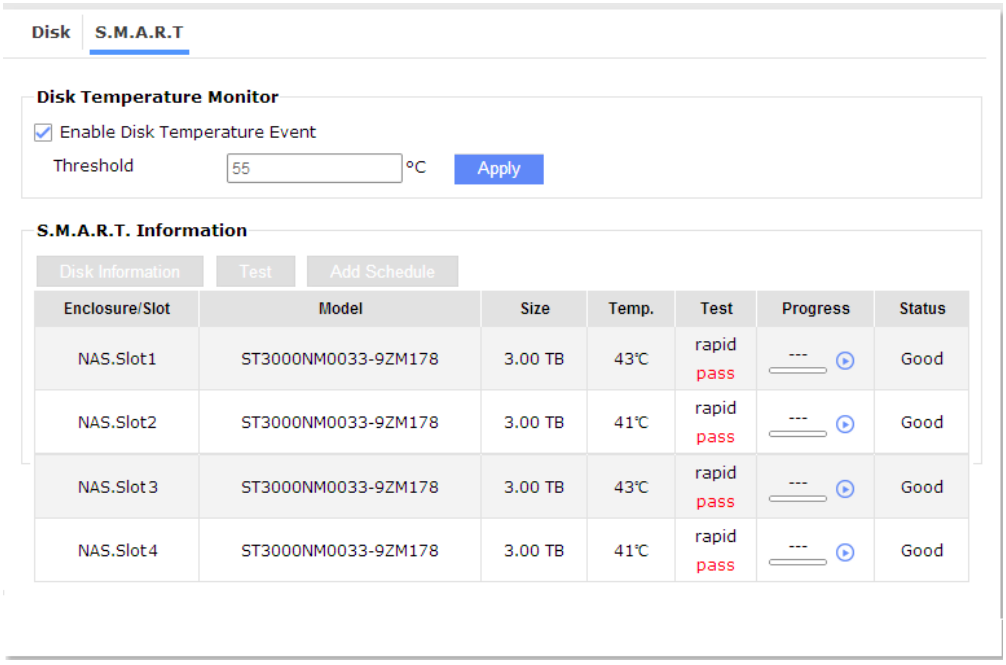
Disk Temperature Monitor

Depending on the ambient temperature of your work environment, you can manually specify an upper threshold for all disk drives in your chassis. If the upper threshold is violated, event messages will be delivered to the administrator.

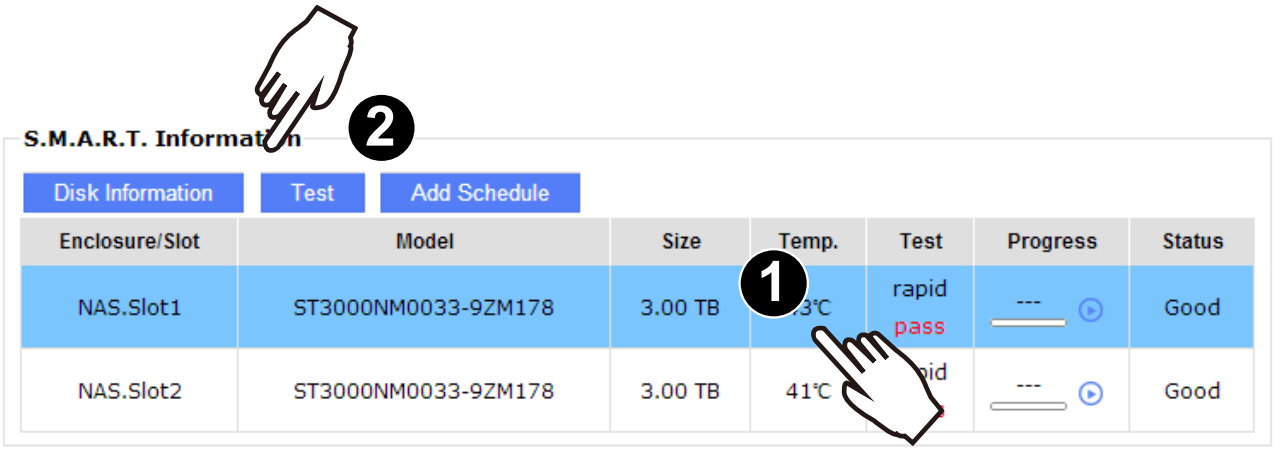
S.M.A.R.T. is short for **Self-Monitoring, Analysis, and Reporting Technology**. S.M.A.R.T. provides near-term failure prediction that monitors pre-determined disk drive attributes that are susceptible to degradation over time. Predictions are limited to the attributes implemented by the HDD manufacturers.

Although attributes are drive specific, a variety of typical characteristics can be identified, for example:

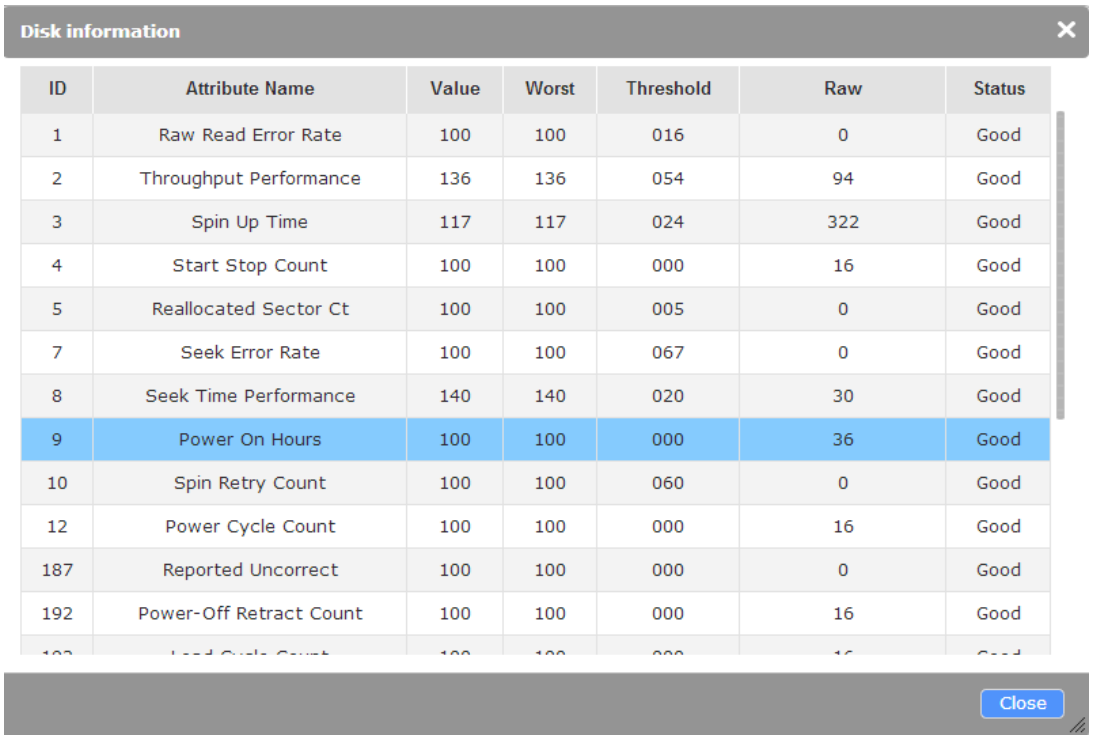
Head flying height, Data throughput performance, Spin-up time, re-allocated sector count, seek error rate, seek time, spin try recount, and drive calibration retry count, etc.



To perform S.M.A.R.T.-related function, click to select a disk drive entry. Once it is highlighted, the tab menu buttons on top will turn blue.

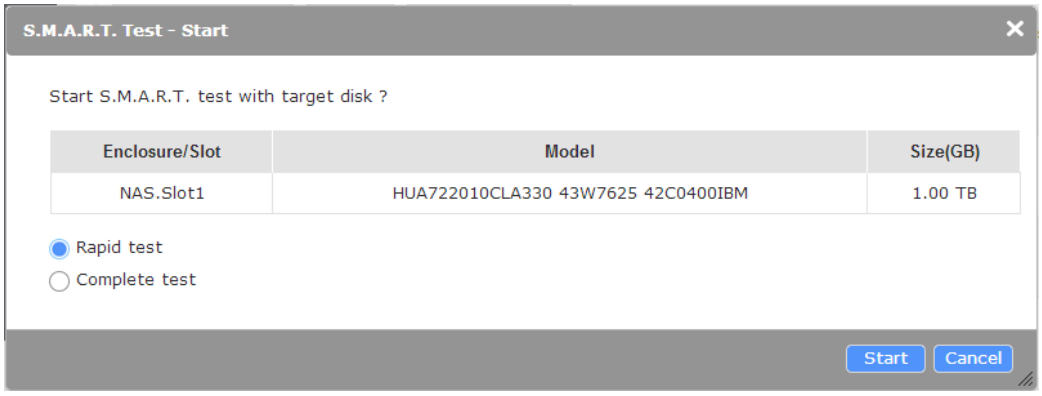


You can click on the **Information** tab to check on the disk drive's working status in terms of its Read Error, throughput performance, spin up time, reallocated sector, etc. These information are listed in the pop-up window.

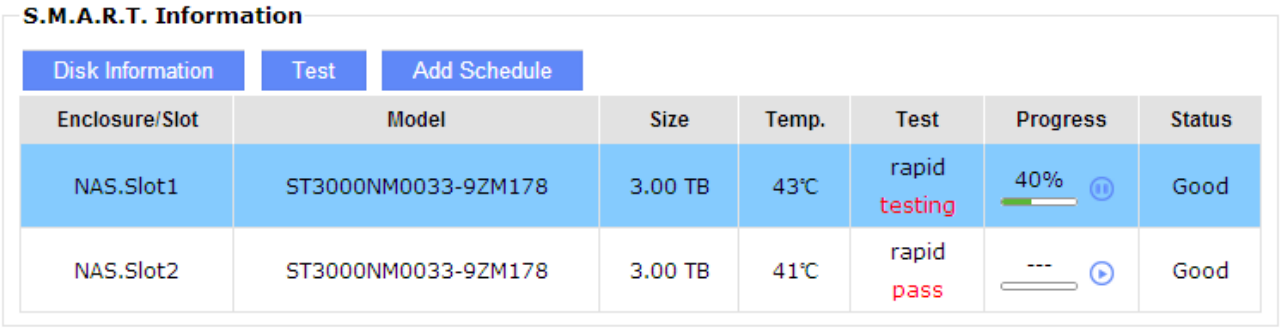

Disk information
ID
Attribute Name
Value
Worst
Threshold
Raw
Status
1 Raw Read Error Rate 100 100 016 0 Good
2 Throughput Performance 136 136 054 94 Good
3 Spin Up Time 117 117 024 322 Good
4 Start Stop Count 100 100 000 16 Good
5 Reallocated Sector Ct 100 100 005 0 Good
7 Seek Error Rate 100 100 067 0 Good
8 Seek Time Performance 140 140 020 30 Good
9 Power On Hours 100 100 000 36 Good
10 Spin Retry Count 100 100 060 0 Good
12 Power Cycle Count 100 100 000 16 Good
187 Reported Uncorrect 100 100 000 0 Good
192 Power-Off Retract Count 100 100 000 16 Good
Close

You can click on the **Test** tab to start a test on disk drives according to the S.M.A.R.T. attributes. You may perform **Rapid Test** or **Complete Test** to acquire the current integrity status. The test utility then polls the hard drives for statuses of the key attributes of its working conditions. The Rapid test checks the electrical and mechanical performance as well as the read performance of the disk. Electrical tests might include a test of buffer RAM, a read/write circuitry test, or a test of the read/write head elements. Mechanical test includes seeking and servo on data tracks. Scans small parts of the drive's surface (area is vendor-specific and there is a time limit on the test). The test checks the list of Pending sectors that may have read errors.

Note that a Complete test will scan through the HDD's disk sectors and will take a long time to complete. A Complete test will take around 3 hours on a 1TB HDD.

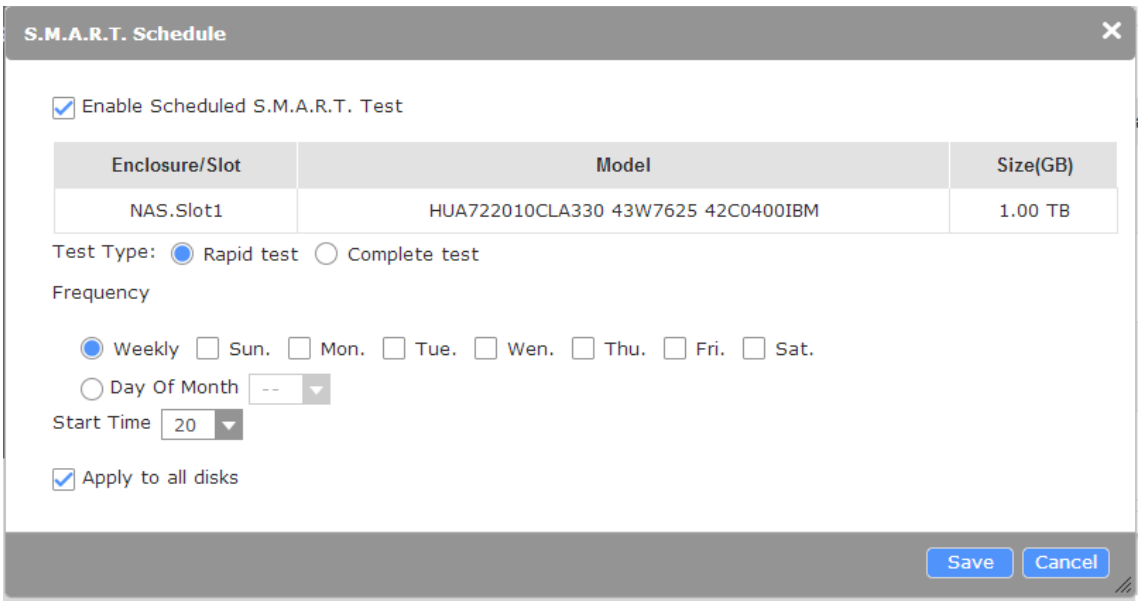


Once the test is started, its progress will be indicated by a small progress bar accompanied by a pause button underneath.



To avoid interruptions to daily services, S.M.A.R.T. test can be scheduled to take place in the off-office hours. For example, you can use the Schedule tool to perform such tests on Sundays.

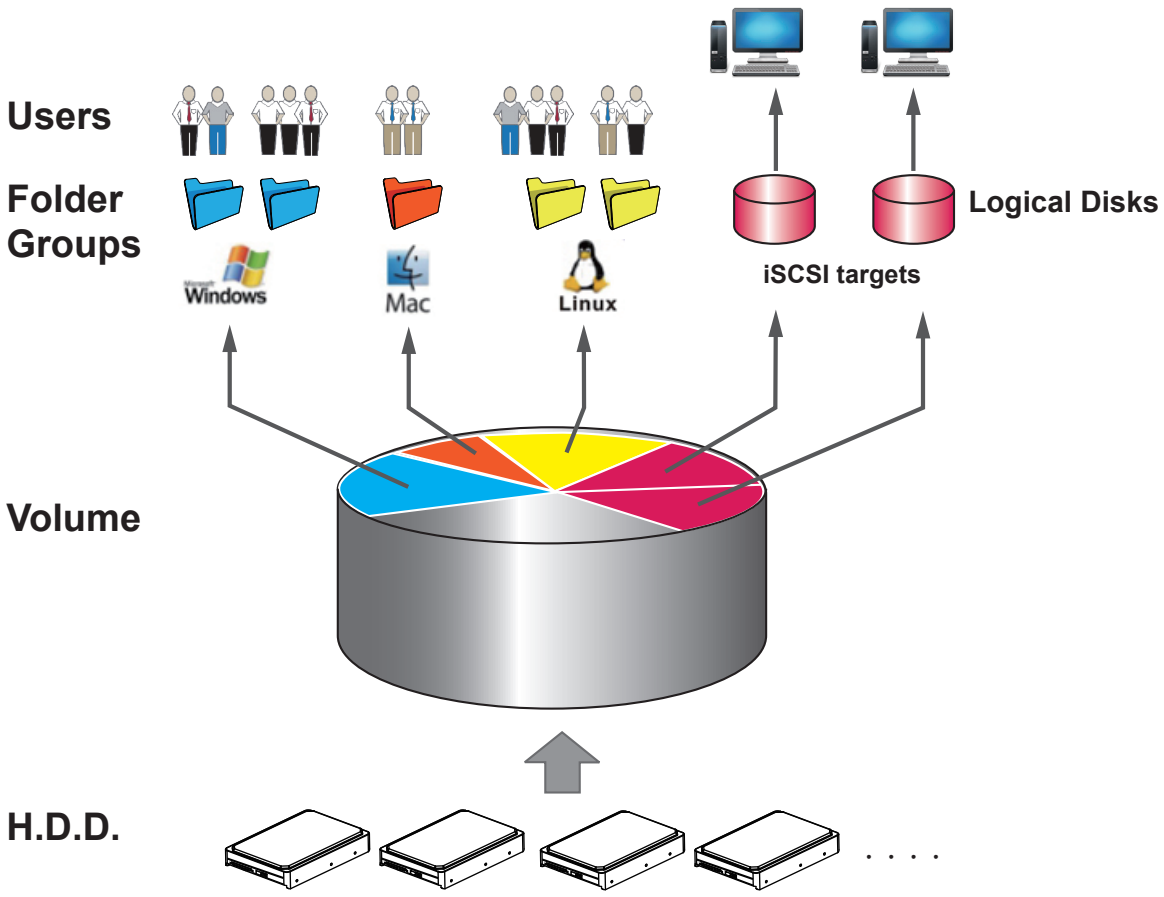
Click on the **Schedule** tab to start the configuration window. Select the Enable checkbox, and configure the time the S.M.A.R.T. test will take place.



4.2. Storage > Volumes

Below is a conceptual drawing showing the physical and the logical elements for sharing storage space to a variety of users/computers. The foundation of the configuration starts from the storage volume that provides fault tolerance, disk capacity, and the combined performance from multiple hard drives.

When a storage volume is ready, you can create logical disks and virtual Folder Groups with their specific attributes for access from different users across the network.

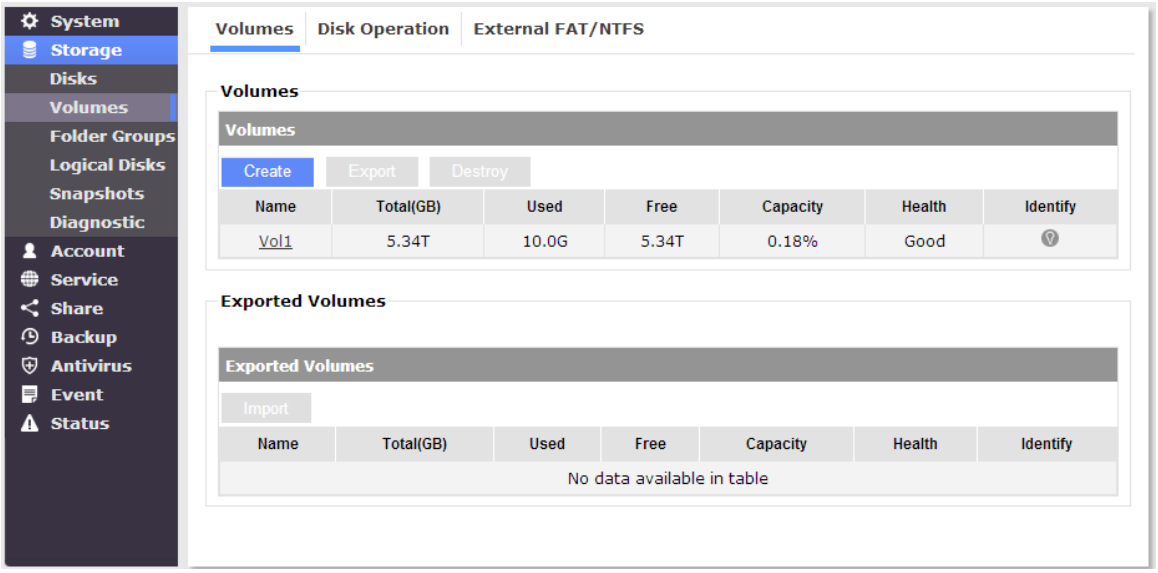


NOTE:

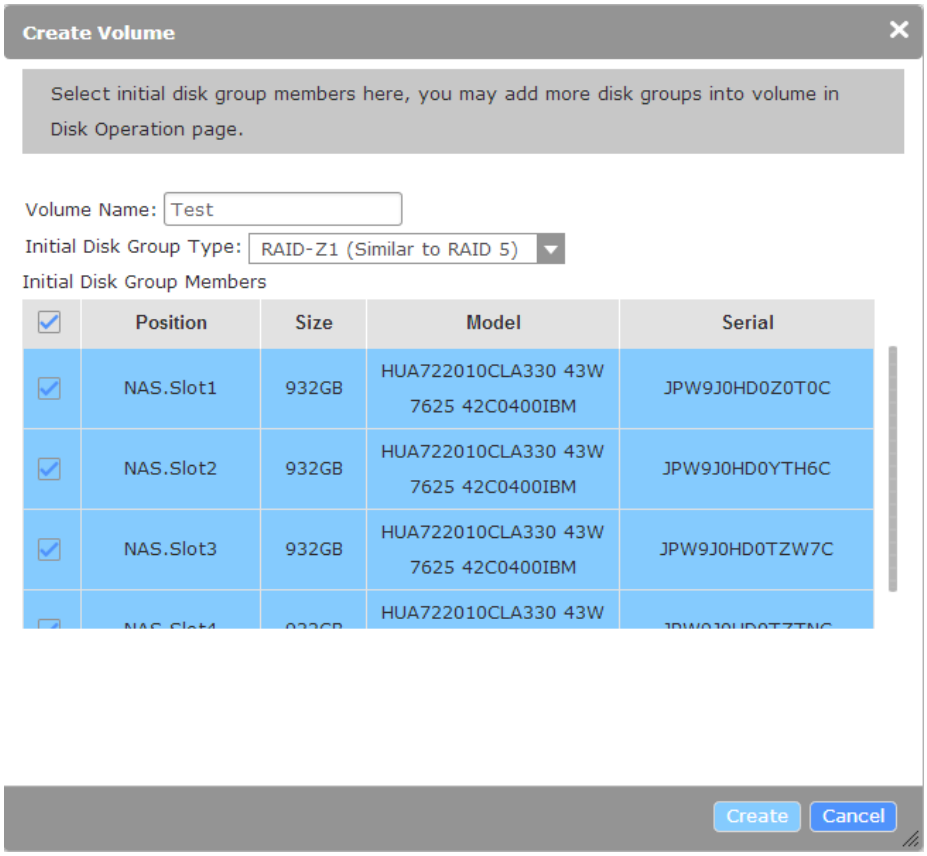
1. The NAS server supports the backup using the Rsync function to USB or e-SATA devices, including USB thumb disk, USB hard disk, or hard disks attached via the e-SATA interface. When the external device is attached to the NAS server, it is automatically mounted. The user can then mount or unmount the USB device.
2. The NAS server supports USB devices formatted in the NTFS or FAT32 format.
3. The 4600U/T series supports external devices via the USB or e-SATA interfaces.
4. The 12600U series supports external devices via the USB interface.

4.2.1 Volumes

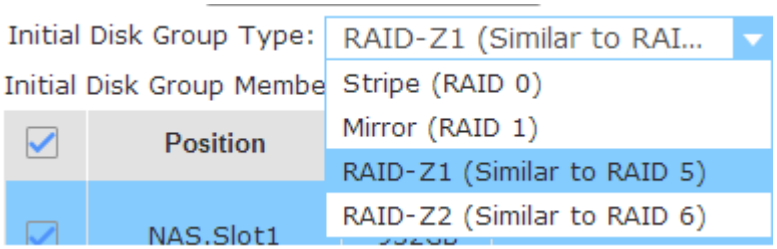
The Storage > Volumes page provides configuration and maintenance for logical volumes that consist of multiple disk drives. Logical volumes provide joint performance and fault tolerance in the event of single or dual disk drive failures.



To create a logical volume,
1. Click on the **Create** button.
2. Enter a name for the volume.



3. Select a Disk Group type from its pull-down menu.

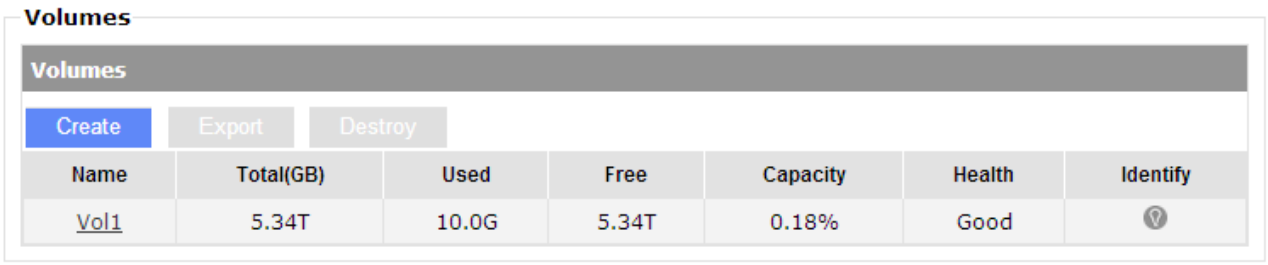


Logical volumes can be shared for users with security control. Below is a summary of volume group types:

RAID 0	RAID level 0 is disk striping only, which distribute data evenly over multiple disks for better performance. It does not provide fault tolerance. RAID level 0 uses two or more hard disks.
RAID 1	RAID level 1 uses disk mirroring, which provides 100% duplication of data. It offers high reliability, but doubles storage cost. RAID level 1 uses two hard disks.
RAID-Z1 (RAID5)	RAID-Z is a higher-level software technology that implements an integrated redundancy scheme in the ZFS file system similar to RAID 5. RAID-Z provides data-protection technology featured by ZFS in order to reduce the block overhead in mirroring. RAID-Z can prevent the RAID 5 "write hole" using the copy-on-write technology; rather than overwriting data. It writes to a new location and then automatically replaces the pointer to the old data. It simply avoids the need for read-modify-and-then-write operations for small writes by only ever performing full-stripe writes. Small blocks are mirrored instead of using parity protection. It is made possible because the file system is aware of the underlying storage structure and can leverage extra space if necessary. RAID-Z2 doubles the parity structure to achieve results similar to RAID 6. Namely, the ability to sustain the failure of two disk drives without losing data.
RAID-Z2 (RAID6)	Similar to RAID 6, The RAID-Z2 can sustain the failures of two disk drives without losing data. It requires at least 3 disk members.

4. Select disk members from the disk drives listed below. The configuration process will be completed almost instantly.

Once created, the volume's information will be listed, including the volume **Name**, **Total capacity (GB)**, **Used** capacity, **Free** capacity, used **Capacity**, and **Health**.



The **Action** button, , lights the disk activity LED of all member drives for identifying the locations of disk members in a chassis.

Export:

A logical volume can be exported for applications such as moving an entire volume (meaning its member disks) to a different enclosure for initializing another system or for backup and test purposes. Once exported, the volume becomes de-activated, and will not receive disk I/Os.

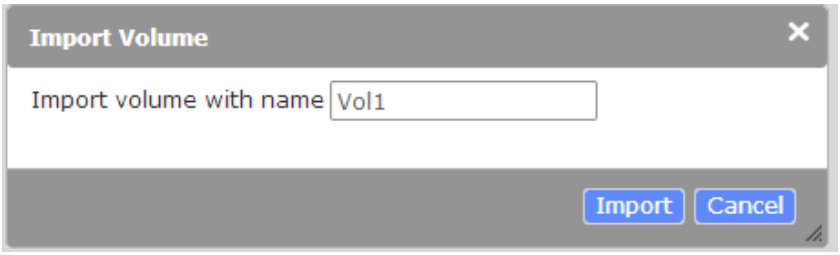
Destroy:

A logical volume is disbanded or destroyed using this button. All data within will be destroyed. Make sure you have backed up all your data before you proceed.

Import:

A logical volume exported from another server can be brought online using this command. Once it is successfully imported, the volume will be ready for I/Os. You should enter the volume name. All directories and device paths are searched. If the device appears to be part of an exported pool, this command displays a summary of the volume with the name of the volume, a numeric identifier, as well as the device layout and current health of the device for each device or file. Destroyed pools, that is, pools that were previously destroyed with the zpool destroy command, are not listed unless other options are specified.

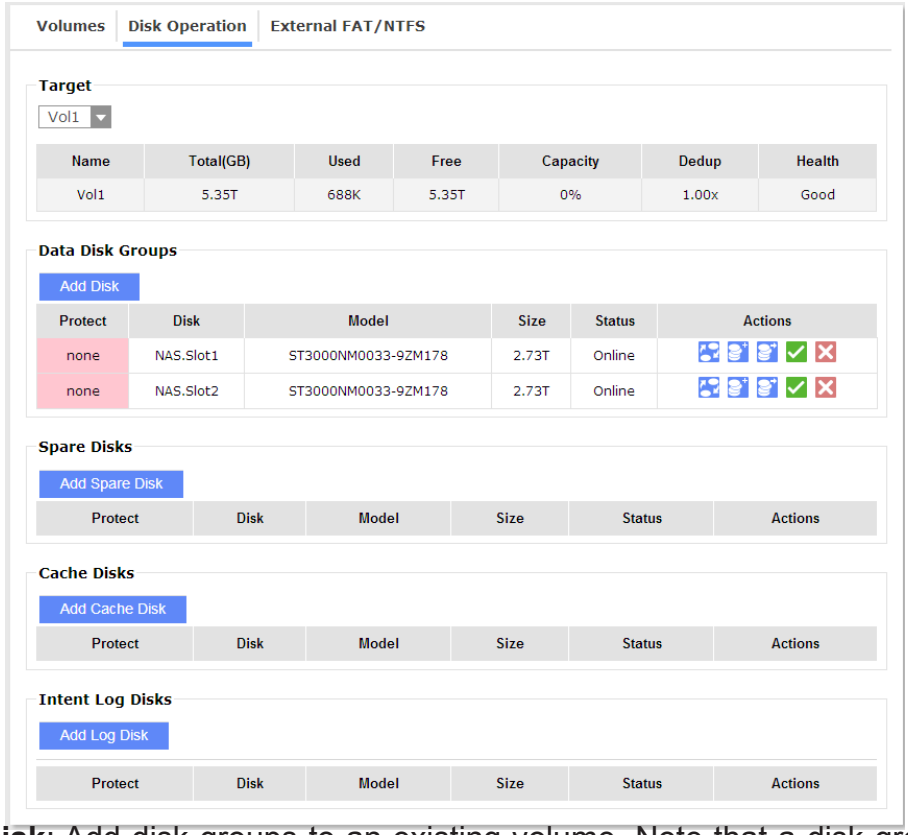
The numeric identifier is unique, and can be used instead of the volume name when multiple exported pools of the same name are available.



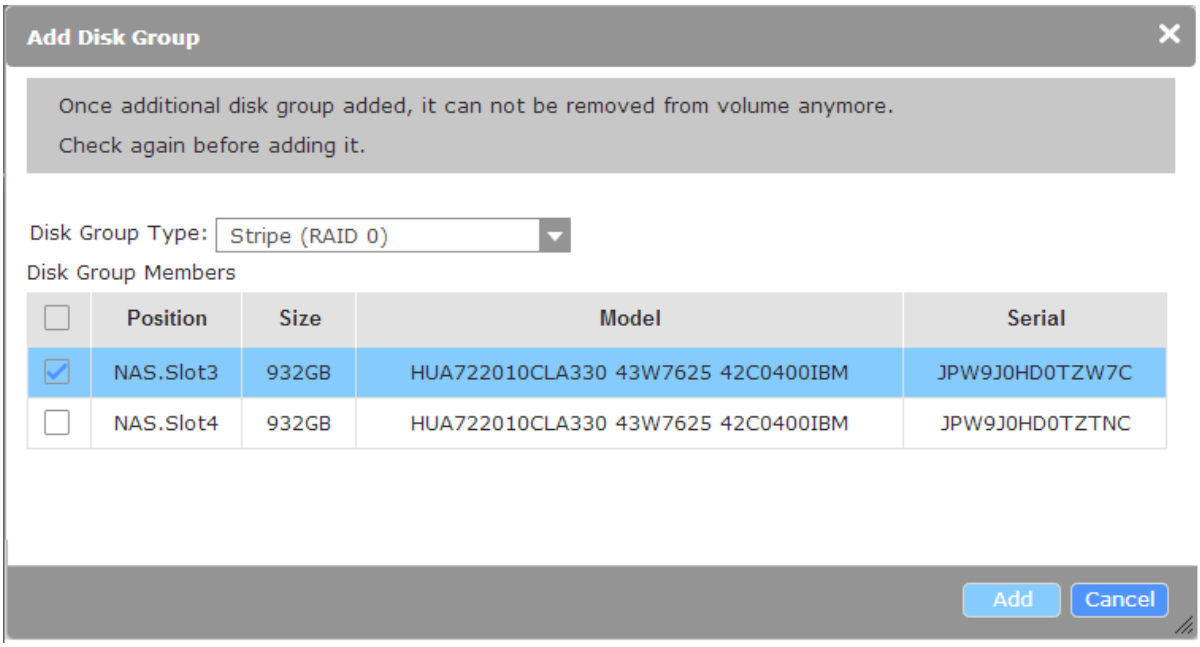
4.2.2 Disk Operation

The Disk Operation page allows you to,

1. **Add Disk**: Add **Disk Group** to an existing volume.
2. **Replace** an existing disk member.
3. **Attach** a new disk member.
4. **Detach** a disk member from a volume.
5. Bring disk member **online** or **offline**.
6. Add a **spare** disk for the volume.



Add Disk: Add disk groups to an existing volume. Note that a disk group thus added can not be removed from a volume. Select the disk drive you prefer and click Add to join it to the volume.



Replace: To replace an existing member disk with another, click on the Replace button.

Select a new disk. Note that an unused drive must be present in your server chassis. Click the **Replace** button. The unused drive must have a capacity larger than the one to be replaced.

The time required to complete the replacement process will depend on the volume size and the size of data kept in the volume.

Attach:

NOTE: The Attach function only applies to RAID0 and RAID1. The Detach function only applies to RAID1.

They do not apply to RAID-Z1 and RAID-Z2 volumes.

To attach new a disk drive to an existing RAID0/1 volume, click on the Attach button in the Disk Groups window. Select from the available disks below, and click the **Attach** button.

When done, the new member will be listed in the Disk Group window.

Detach:

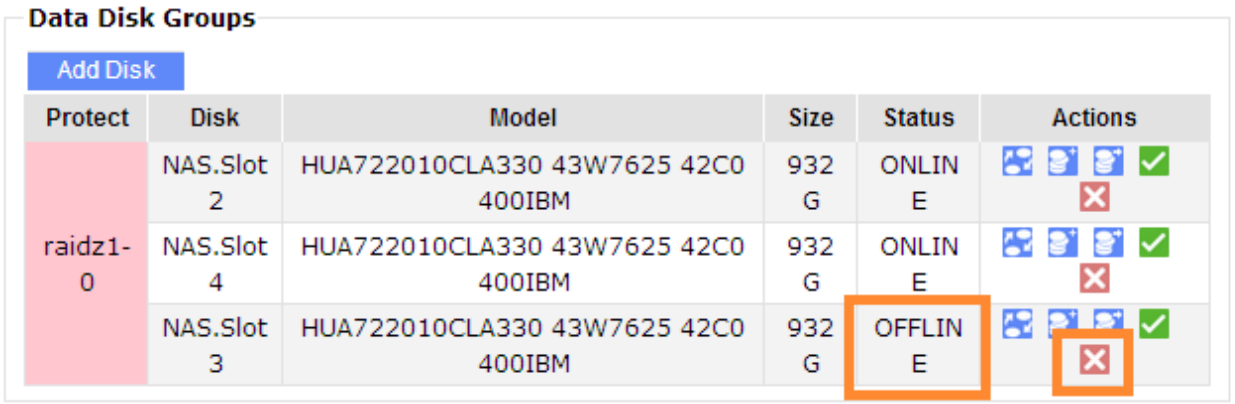
NOTE: The **Attach** functions only apply to **RAID0** and **RAID1**. The disk **Detach** function only applies to **RAID1**. They do not apply to RAID-Z1 and RAID-Z2 volumes

To detach a member disk drive from an existing RAID1 volume, click on the **Detach** button in the Disk Groups window. A confirm message box will appear. Click **Detach** to proceed.

Online & Offline:

The **Offline** mode is mainly designed for you to perform the replacement task. A disk can be changed to the Offline mode, so that you can replace a faulty member disk. When the faulty member is replaced, system will automatically resilver the disk status. The **Online** and **Offline** functions allow you to temporarily disband or re-join a member disk from the storage volume.

Note that if you set an active disk drive to the Offline status, you can replace a faulty disk drive.



The following functions are available for the 12600 series:

Add Cache Disk: The 12600 series supports the Cache Disk function. The cache disk function manages buffer memory resources to acquire, manage, and release limited memory resources. Using an SSD disk as the cache memory, with its larger capacity, the buffer memory for the file system can be significantly expanded.

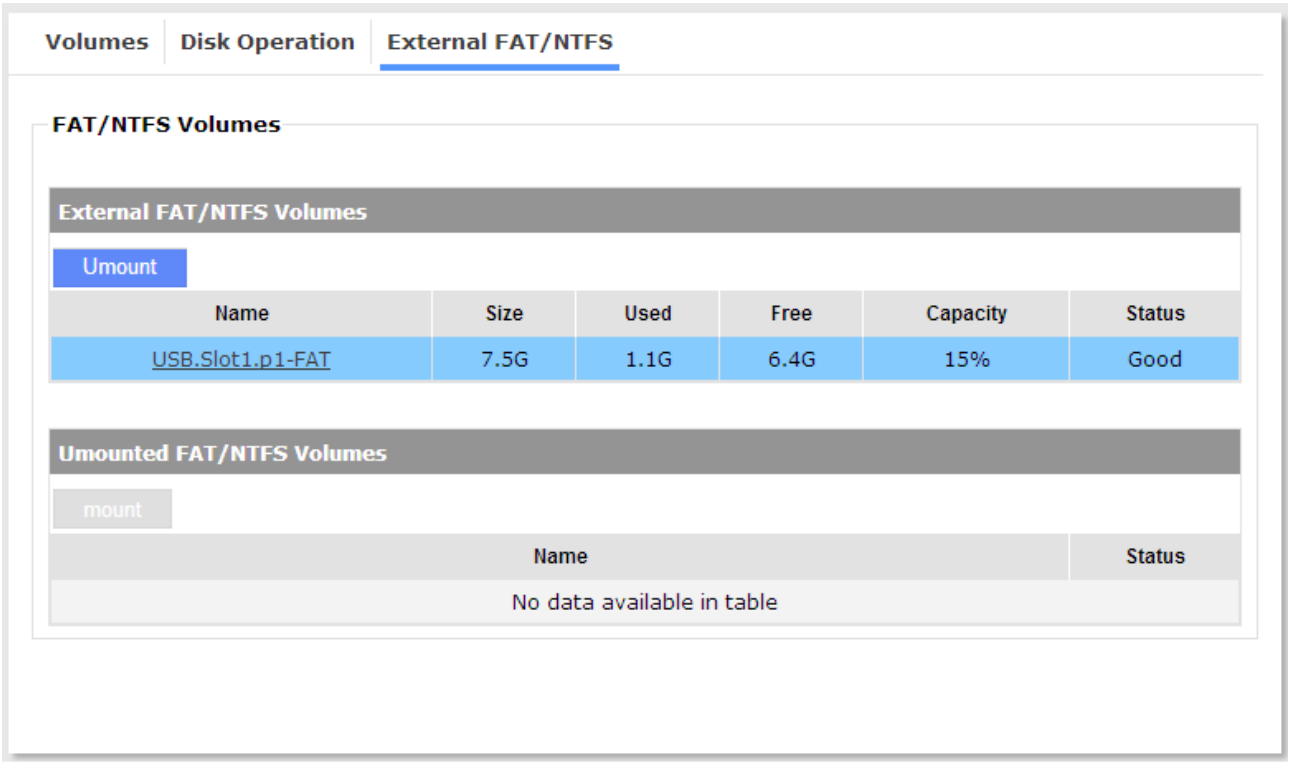
Once data is read into the system's main memory ARC, a replica is immediately placed at the SSD ARC. Once the data needs to be read once again, data can be rapidly retrieved from the SSD ARC (also known as the L2 ARC).

Add Intent Log Disk: The Intent Log index record keeps the transaction record using an added SSD disk. The file system utilizes this methodology to facilitate data writes, while maintains the safety of files in the event of file system crash.

Due to the fact that writing these intent log can also consume system resources, these log can be written to a separate SSD disk in order to avoid impact to the disk read/write performance.

4.2.3 External FAT/NTFS

This window allows access to external devices, such as USB drives, formatted in the Windows FAT and NTFS format. These external devices can be mounted and unmounted using the onscreen functional buttons. You can click on the name entry to directly access the files or folders contained within.

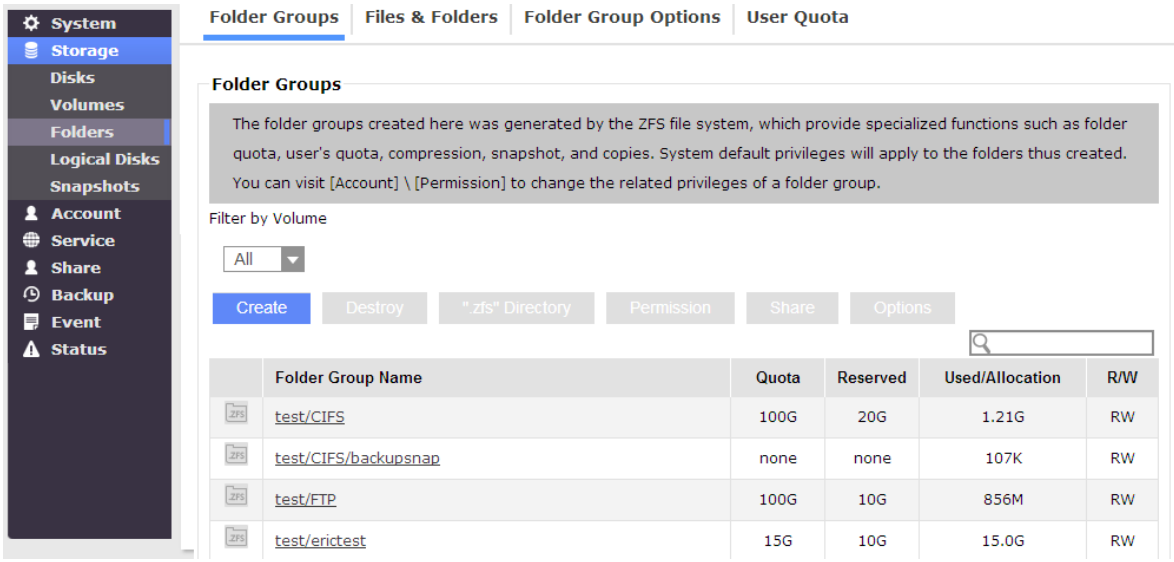


4.3 Storage > Folder Groups

4.3.1 Folder Groups

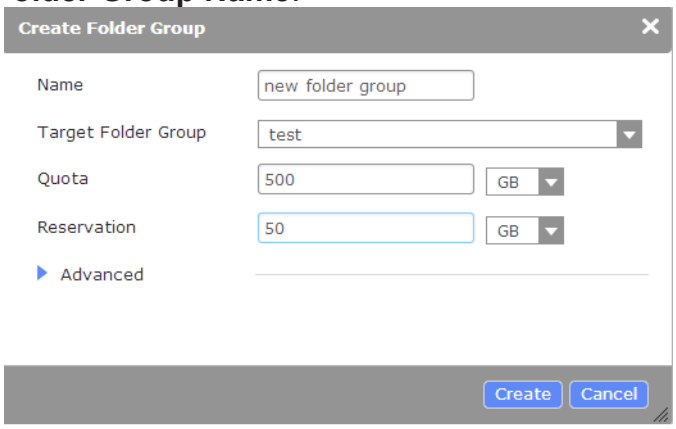
The Folder Groups created here are generated by the NAS server file system, which provide specialized functions such as folder quota, user's quota, compression, snapshot, and copies. System default privileges will apply to the Folder Groups thus created. You can visit **Account** > **Permission** to change the related privileges of a specific Folder Group.

You can share a specific Folder Group in a volume in the NAS server with other users on the network. When you create a share, you can assign the access permission to the share with access rights for other users as well.

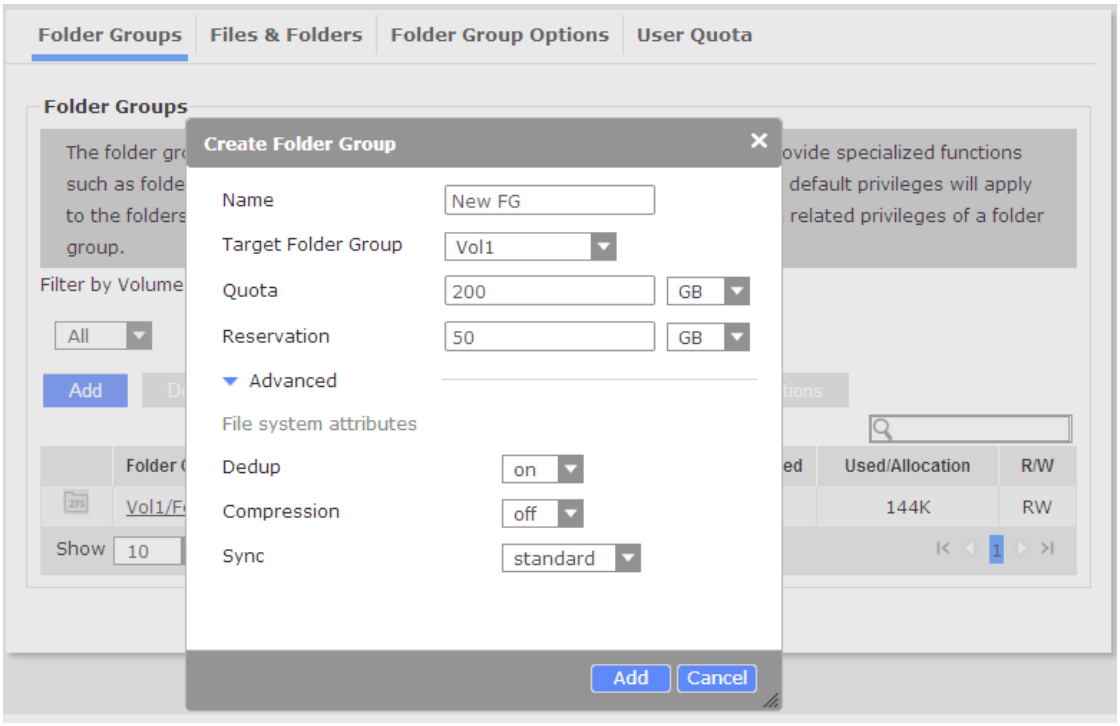


To create a Folder Group

1. Go to **Storage** > **Folder Groups**.
2. Select a volume from which you want to create a Folder Group.
3. If you want to create a new share under an existing Folder Group, select an existing Folder Group from the **Target Folder Group** drop-down list. Otherwise, select the storage volume itself. An example can look like this: volume/test/sub-folder.
4. If you want to share a new Folder Group under a volume, simply select an existing volume from the Target Folder drop-down list.
5. Enter a new **Folder Group Name**.



6. Enter a capacity number in Gigabytes as the share **Quota**.
7. Enter a capacity number in Gigabytes as the **Reserved** capacity which is actually allocated space claimed from the storage volume.
8. You can click on the **Advanced** tab to open the advanced option menu. Here you can select to enable the **Synchronized** option as **Standard** or **Always**. The **Sync** option indicates whether the Folder Group will be synchronized by the system's synchronous requests. Because of the system's copy-on-write characteristics, the synchronization dos not consume system resources.
9. When done, click on the Create button.



NOTE:

1. The 4600U/T series does not support Dedup and Copy functions.

2. Deduplication is the process of eliminating duplicate copies of data. Dedup is generally either file-level, block-level, or byte-level. Chunks of data -- files, blocks, or byte ranges -- are checksummed using some hash function that uniquely identifies data with very high probability.

Chunks of data are remembered in a table of some sort that maps the data's checksum to its storage location and reference count. When you store another copy of existing data, instead of allocating new space on disk, the dedup code just increments the reference count on the existing data. When data is highly replicated, which is typical of backup servers, virtual machine images, and source code repositories, deduplication can reduce space consumption not just by percentages, but by multiples.

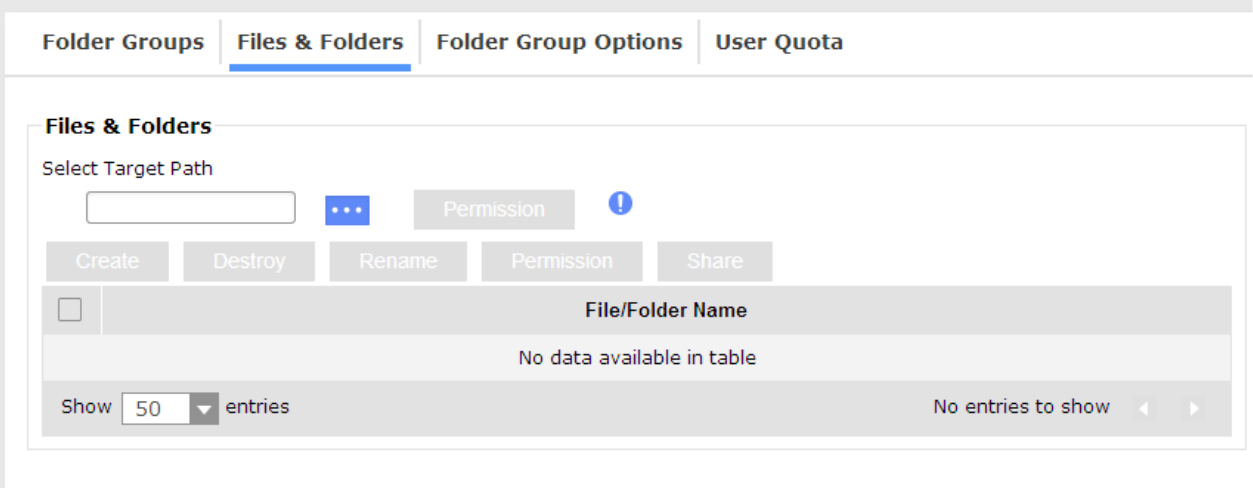
The "ZFS directory" tab allows you to directly see the snapshot backups of a folder group in a system-embedded snapshot container. However, when doing so, Windows file manager will have troubles calulating the volume capacity of this folder group.

The Permission tab guides you to the Permission configuration window, about who can access the folder group.

If you should need to remove an existing Folder Group, click to select a Folder Group, and then click on the **Destroy** button.

4.3.2 Storage > Folder Groups > Files & Folders

Select a target folder ••• before making configuration changes.



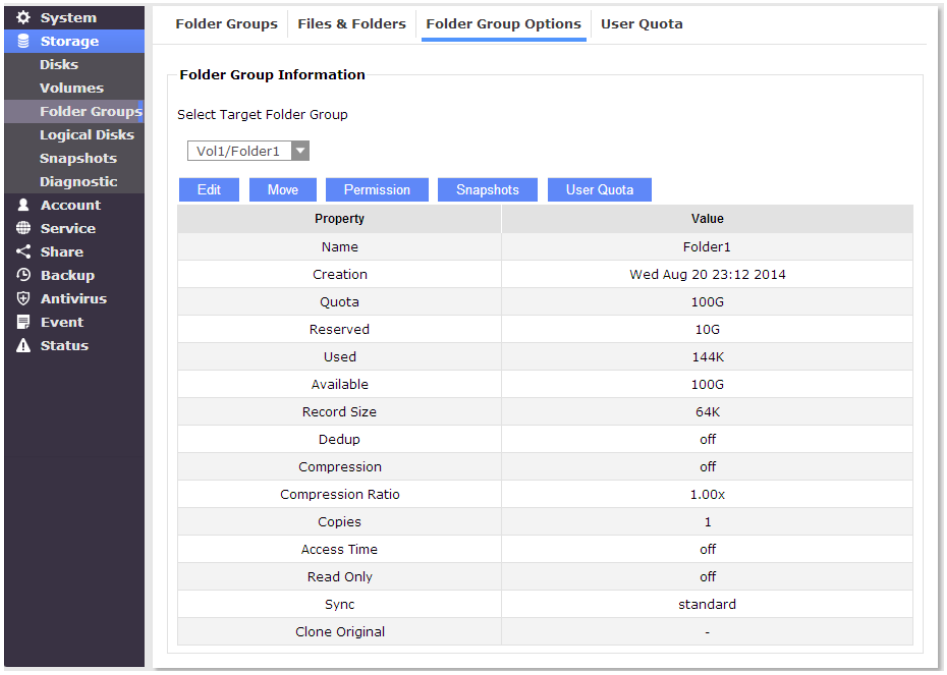
The Create and Destroy button allow you to create or remove a sub-directory under the directory you selected.

The rename tab allows you to rename the target folder or file.

The Permission tab guides you to the Permission page, and the Share tab allows you to directly share the sub-directory to computers running different operating systems.

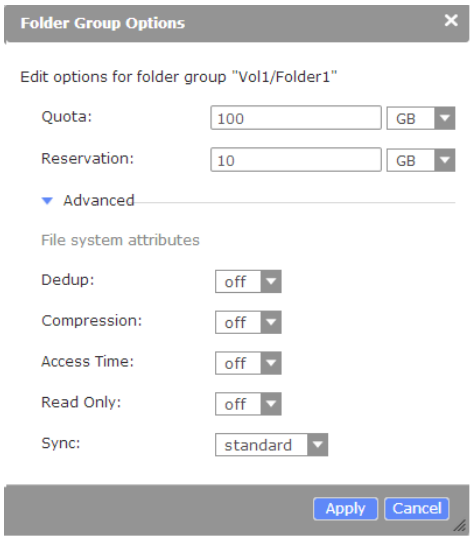
4.3.3 Storage > Folder Groups > Folder Group Options

You can go to the details of a shared Folder Group using the Edit, Move, Permission, Snapshots, and User Quota tabbed menus.



Before you begin any configuration, select a target Folder Group using the **Select Target Folder** menu.

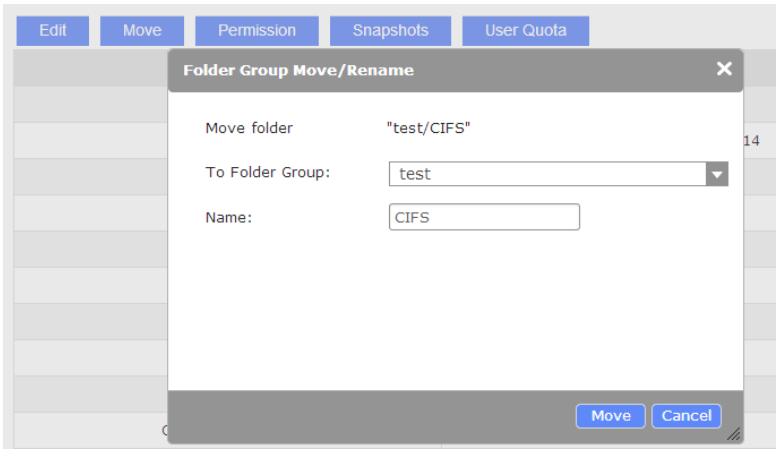
1. **Edit**: Click this button to edit the following attributes such as storage **Quota**, **Reservation**, **Access Time**, **Read Only** rights, and so on.



NOTE:

- The 4600U/T series does not support the Dedup and Copy functions. Neither can you disable the the Sync function using the 4600U/T series.
- The 4600U/T supports the Compression function.
- The Copy function is not available on the 12600U series.

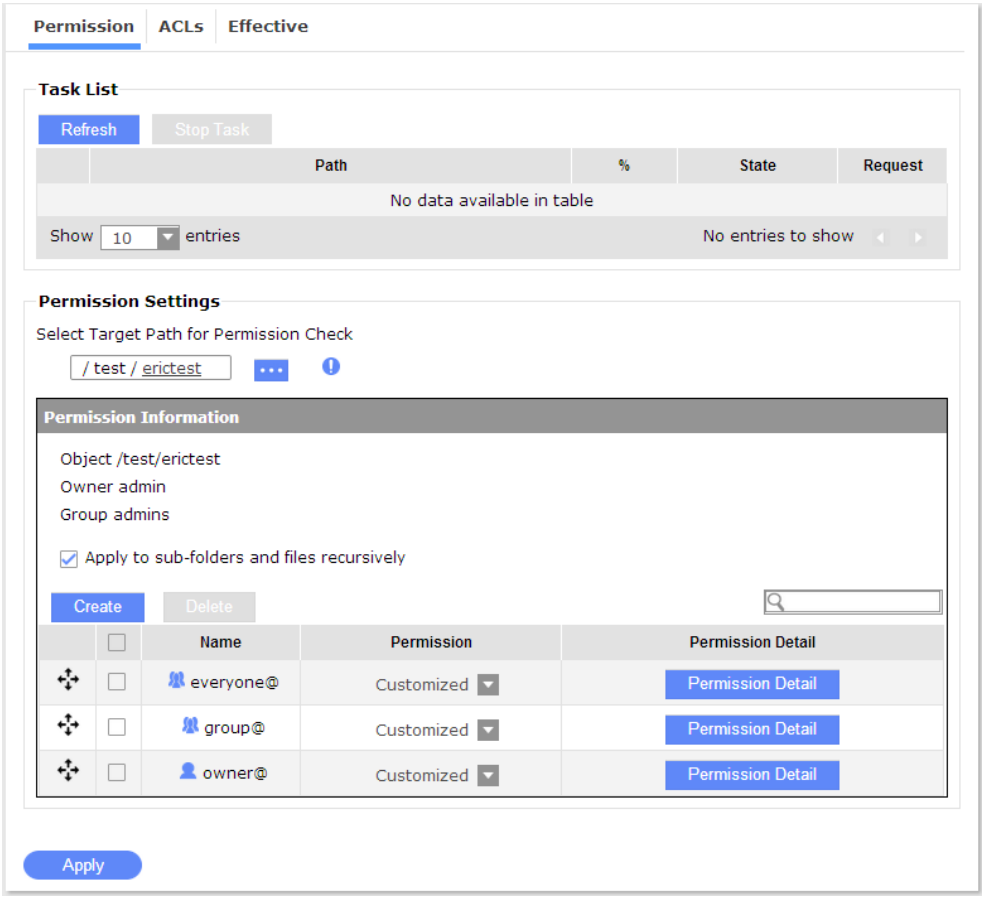
2. **Move**: You can move an existing Folder Group to a different location on the directory hierarchy.



3. **Permission**:

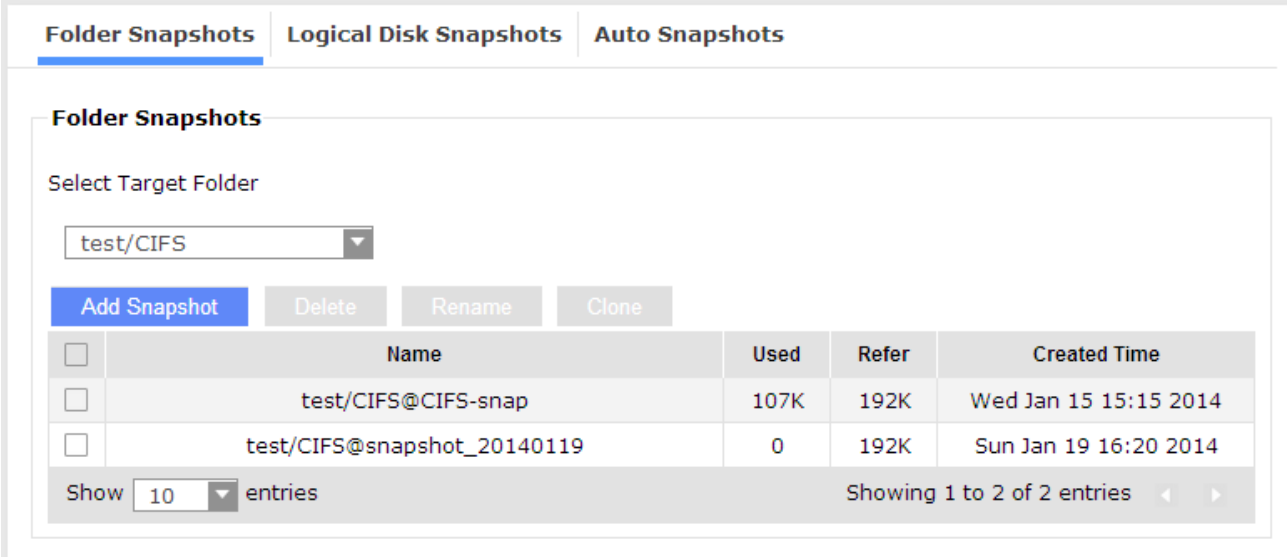
3-1. Select an existing Folder Group.

3-2. Click on the **Permission** tab. The system will direct you to the **Account** > **Permission** page. From there, you can create new account, or select Owner, Group, or the Everyone permission for the access to the particular Folder Group.

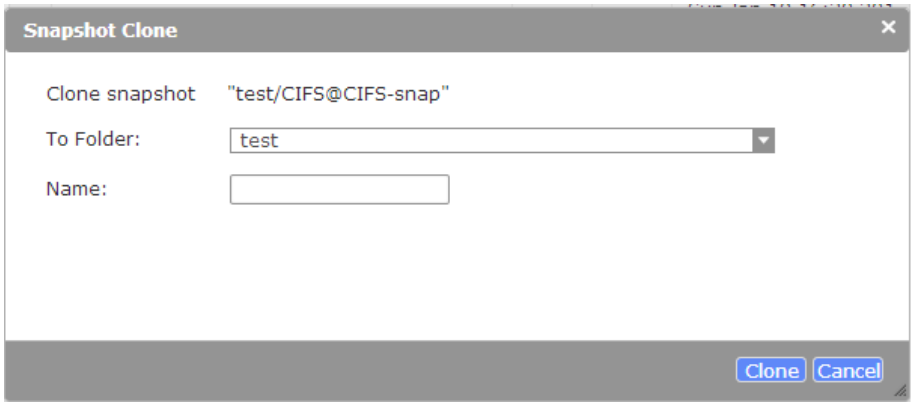


4. **Snapshots**:

Click on the Snapshots tabbed button will direct you to the Storage > Snapshots window. Please refer to page 97 in the later discussion.

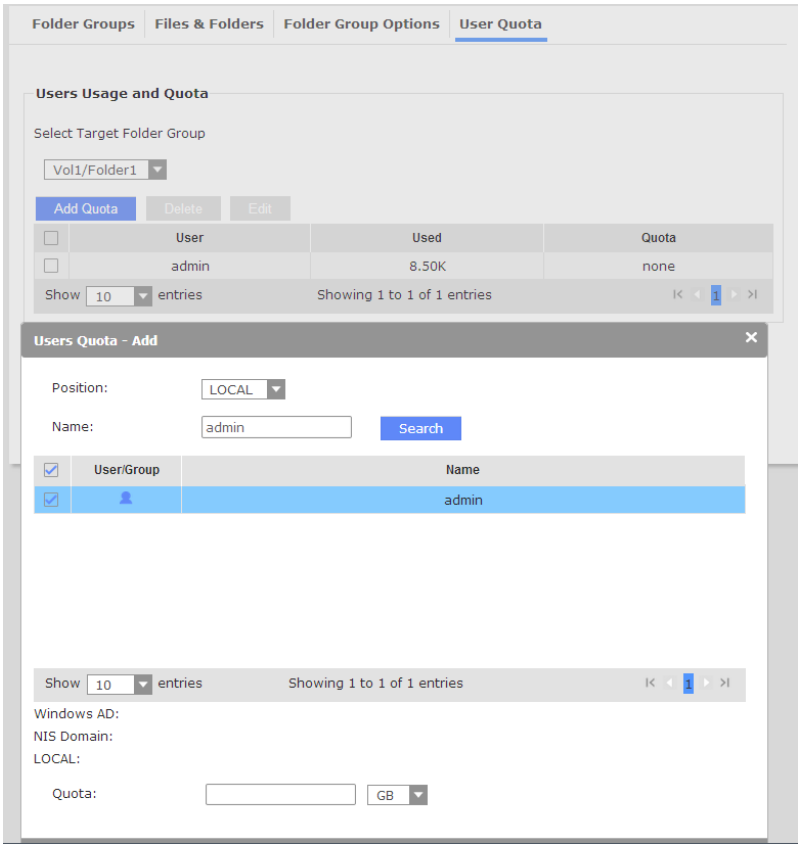


Once a snapshot is created, click on an existing snapshot and click the **Clone** button. You can then clone the snapshot backup to a local Folder Group for data analysis or for the purpose of backup to a different location.



4.3.4 Storage > Folder Groups > User Quota

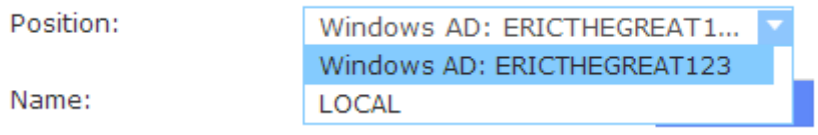
From here, you can create a user quota (designated usable storage use) for a user's leverage. You can create the **Add Quota** button to open the **Users Quota** window.



Click on the **Position** pull-down menu to display the **Local** or **domain name** (if you already joined the server to one of the Windows AD or NIS domain).

Enter a user name in the **Name** entry and click on the **Search** button to look for a user that you imported from a domain server (that already resides in the domain).

You can then enter a storage space size in the **Quota** entry field, e.g., 100GB from the pull-down menu. .

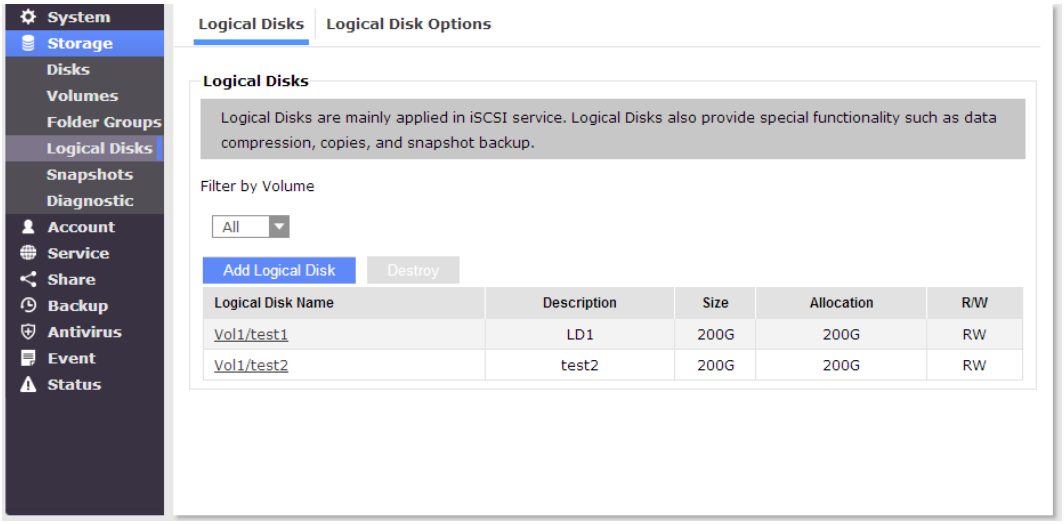


NOTE:
This window directs you to the next tabbed window, **User Quota**.

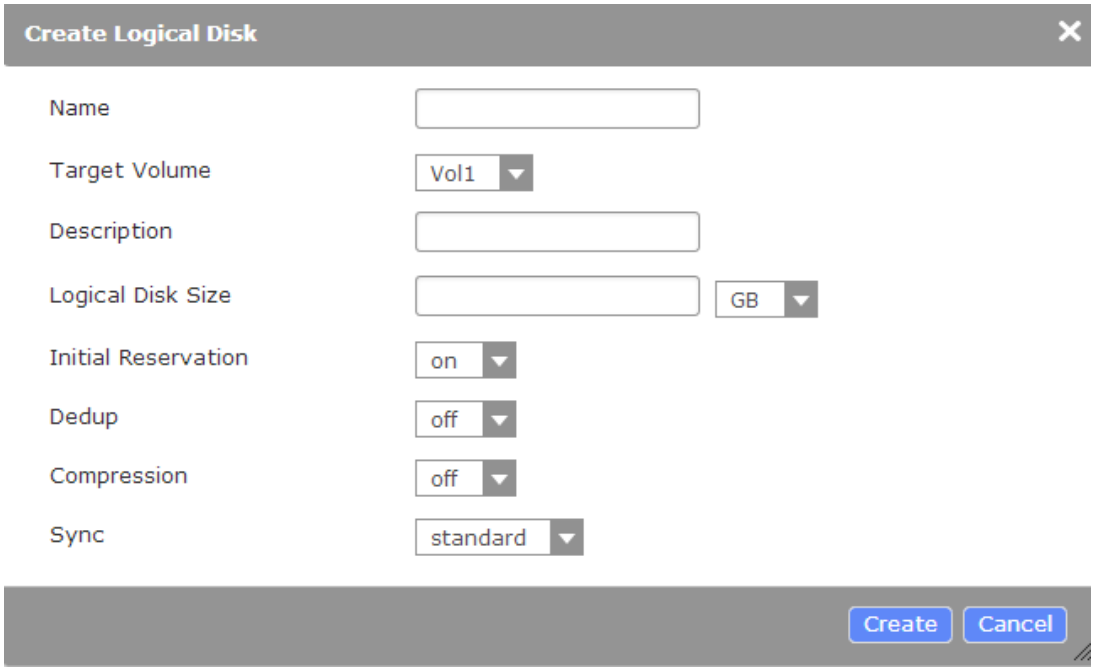
4.4. Storage > Logical Disks

Logical Disks are mainly applied in iSCSI service. Logical Disks also provide special functionality such as data compression, copies, and snapshot backup. By carrying SCSI commands over IP networks, iSCSI is used to facilitate data transfers over intranets and to manage storage over long distances. iSCSI can be used to transmit data over local area networks (LANs), wide area networks (WANs), or the Internet and can enable location-independent data storage and retrieval.

Logical Disks are the storage spaces separately segregated for being shared over the network as iSCSI targets. This page creates the storage spaces for use as described in page 117 - **Service** > **iSCSI Targets**. .



1. To create a space as an iSCSI target, click the **Add Logical Disk** button.
2. Create a name for the Logical Disk, Note that space and special characters are not supported in this field.



3. Select a Volume from which you want to create a Logical Disk.
4. Enter a description for the Logical Disk, such as "iSCSI target for PC #xx."
5. Enter and/or select a storage space as the Logical Disk Size.
6. Select to preserve a certain amount of disk space as the Initial Reservation.
7. Select the Compression option.
8. Select how many snapshot copies will be preserved in your storage volume.
9. Sync: see the next page for the choices.

Standard
This is the default option. Synchronous file system transactions are written out and then secondly all devices written are flushed to ensure the data is stable (not cached by device controllers).

Always
This ensures file system transaction is written and flushed to stable storage by a system call return. Selecting this option can bring performance penalty.

⚠ **IMPORTANT:**

- The 4600U/T series does not support the Dedup and Copy functions. Neither can you disable the the Sync function using the 4600U/T series.
- The 4600U/T supports the Compression function.
- The Initial Reservation (Thin Provisioning) function applies to the 12600 series, not the 4600 series.
- The Copy function is not available on the 12600U series.

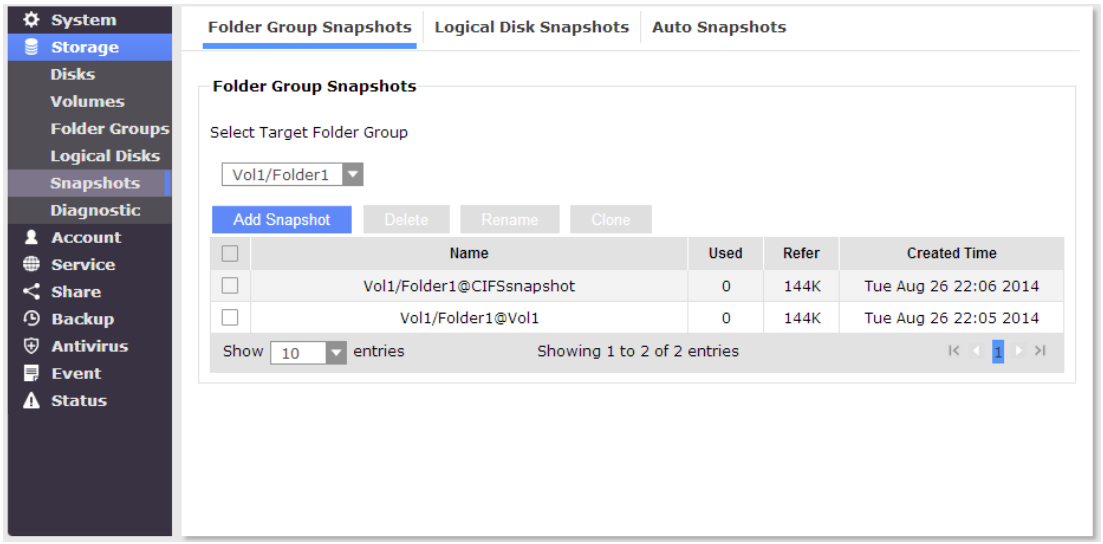
4.5. Storage > Snapshots

Snapshots are read-only, point-in-time preservations of a file system or a portion of a volume. Because the server runs on a copy-on-write operating system, snapshots can be taken almost instantaneously.

Folder Group Snapshots

To create snapshots for a Target Folder Group, select a Folder Group under the major storage volume from its pull-down list. Click the Add Snapshot button.

You can then specify a Name for the snapshot. You can select the Recursively check box to enable snapshots for all sub-directories under the currently selected Folder Group.



Logical Disk Snapshots

To create snapshots for a Logical Disk, select a logical disk under the major storage volume from its pull-down list. Click the Add Snapshot button.

You can then specify a Name for the snapshot.

Auto Snapshots

Easy Add: The Easy Add button brings forth a scheduler tool, where you can configure an Hourly, Daily, Weekly, or Monthly schedule according to which snapshots will be automatically taken.

You can designate a Life Time for the snapshots thus taken.

Add Snapshot: The Add Snapshot button brings forth a scheduler tool, where you can configure an Hourly, Daily, Weekly, or Monthly schedule for target Folder Groups or logical disks.

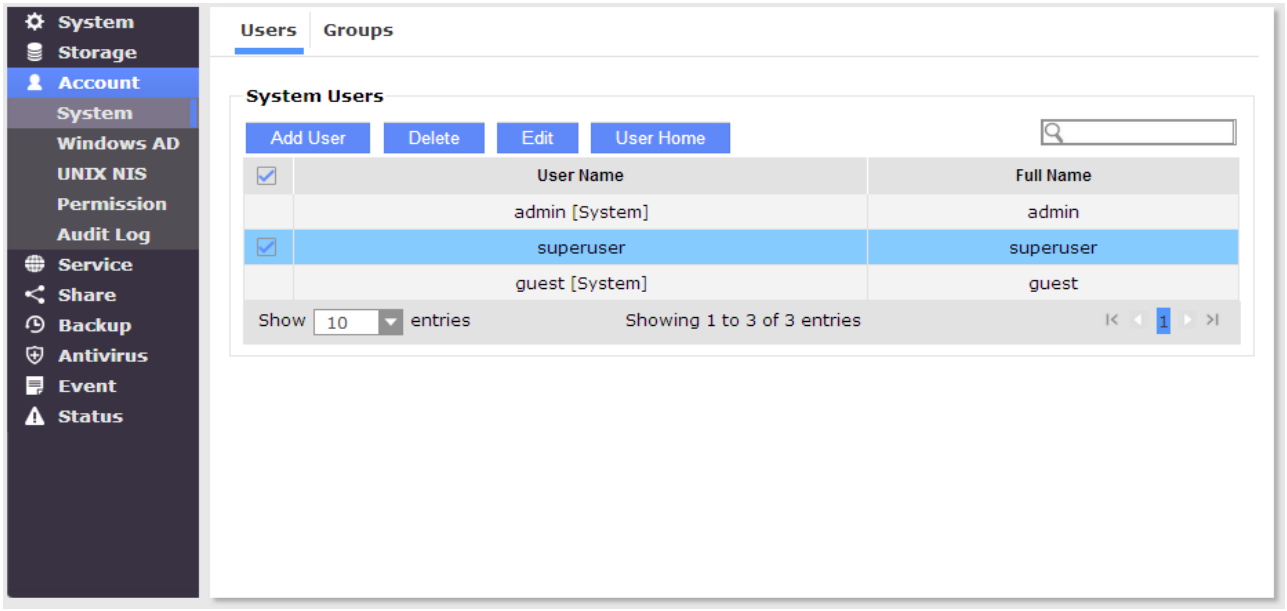
All snapshots taken will be listed. You can click **Delete**, **Edit** to configure the existing schedules, or select **Recursively** to include sub-directories.

Chapter 5 Account

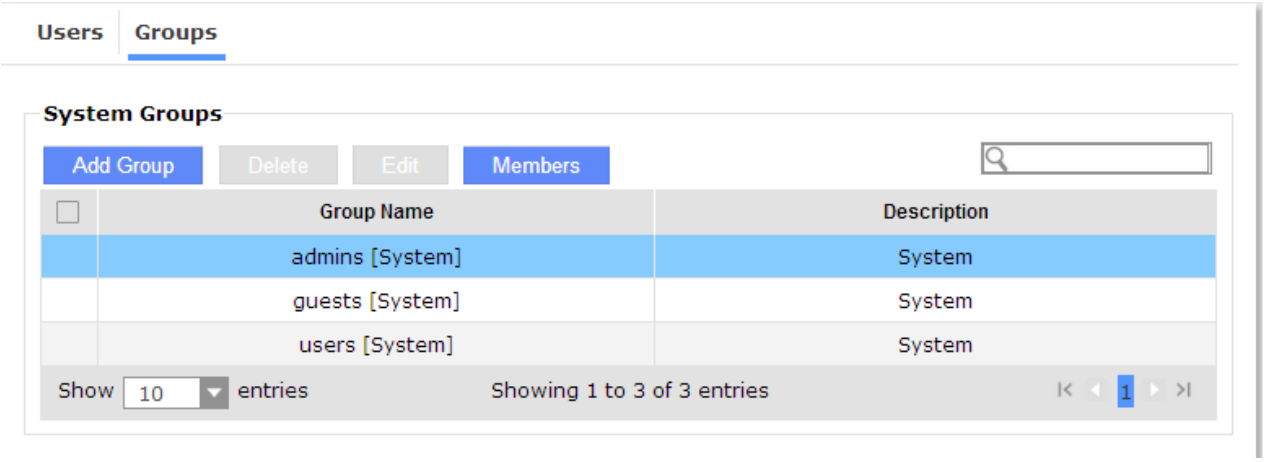
The Account windows allows you to create local or domain accounts for Windows AD or Unix environments. The windows also provides access to control the permission list and access privileges.

5.1. Account > System

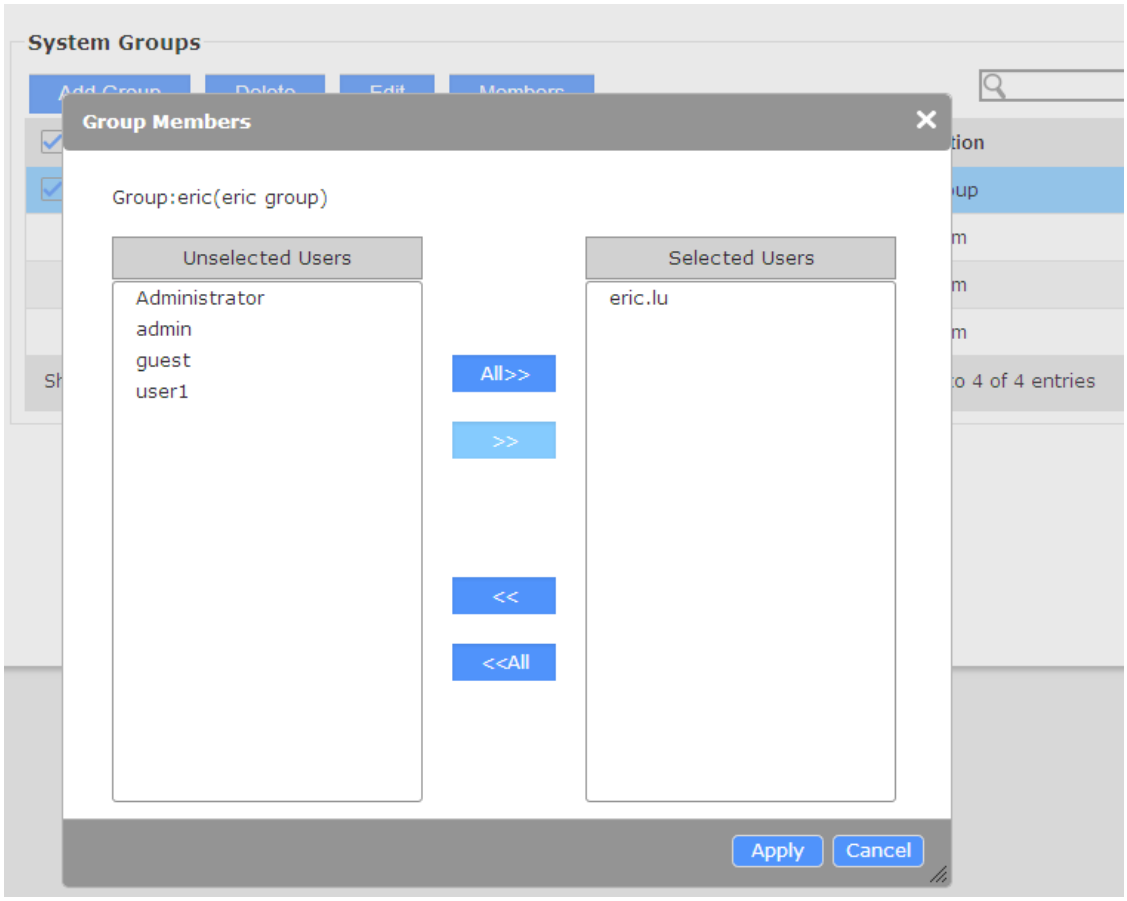
The System page provides access to current users' configuration and allows you to create new users, or to delete or edit the current users.



The Groups window provides access to current user groups. The default local groups include **admins**, **guests**, and **users**. You can Add new groups and edit their privileges. Note that you can not edit privileges for users in the default groups.

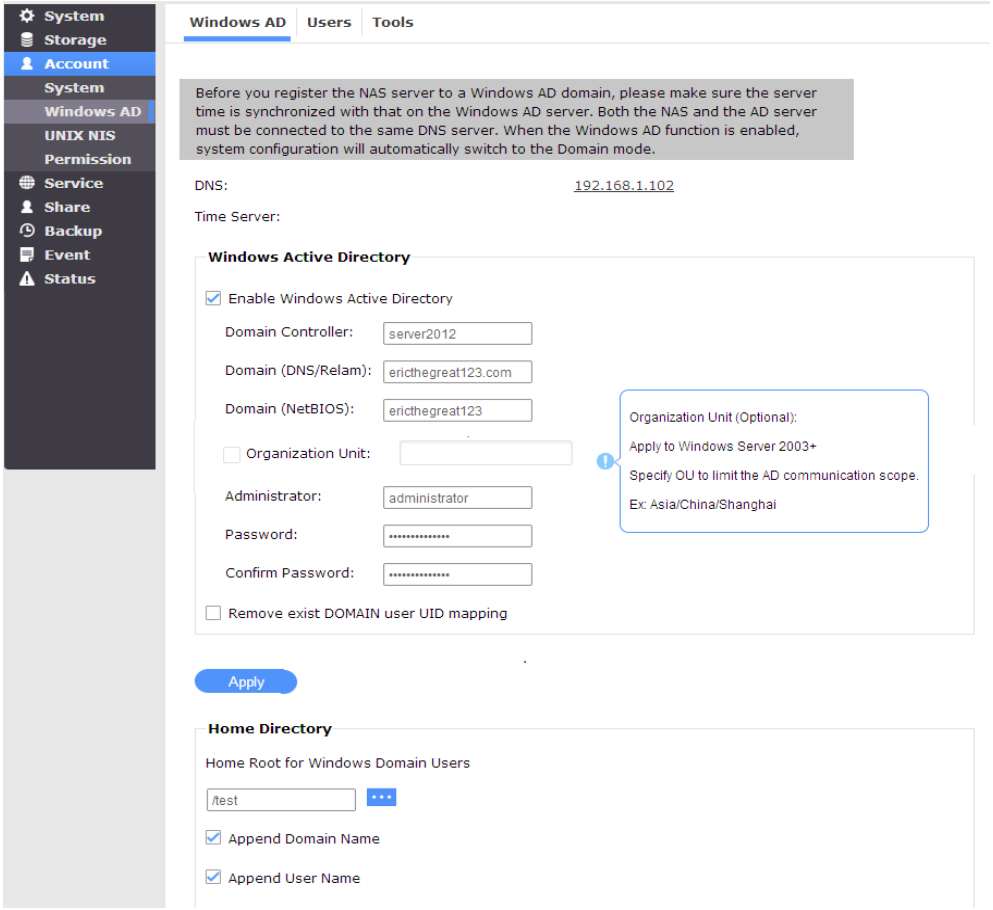


The Members window allows the administrator to move users among different privilege groups using the various move buttons. You can recruit or disband users from each specific group.



5.2. Account > Windows AD

Active Directory (AD) is an implementation of LDAP directory services by Microsoft for use primarily in Windows environments. The AD functions as the provider of central authentication and authorization services for Windows-based computers. In addition, Active Directory supports deploying software and assigning policies on a organizational hierarchy.



In workgroup mode, the SMB/CIFS service is responsible for authenticating users locally when access is requested to shared resources. In domain mode, the SMB/CIFS service uses pass-through authentication, in which user authentication is delegated to an Active Directory domain controller. Independently of whether you will use the SMB/CIFS for anonymous access, non-anonymous (workgroup)or in domain mode, the very first step is to configure SMB/CIFS server. You can simply review and accept built-in system defaults. The rest of this Section includes:

Note some of the environment related requirements:

1. **Time** (namely, the time server settings) must be accurate between AD server and the NAS server.
2. **DNS** servers, **NetBIOS**, and **domain** values have to match those on the AD server.

   For example, you should check on System > Network, to ensure the NAS server is joined into same network as the AD server. The DNS server in the network can be pointed to the same physical address of the AD server.

Please note the following: to join an AD domain, the server must be setup so that the Active Directory Domain and the server are in the same DNS Domain. In general, one key element in the Active Directory functionality is its DNS infrastructure. You can refer to Microsoft Knowledge Base article - "Troubleshooting Active Directory—Related DNS Problems." The problems may include DNS server and zone configuration, and presence of DNS domain controller locator records (SRV records).

Optionally, you can add users/groups that will use this shares on this server and will perform join operation. Check on Account > Permission, type in user (or group) name that are identical to those setup on the Windows AD server.

To join a **Windows Active Directory**:

1. Select the Enable Windows Active Directory checkbox.
2. Enter the Domain Controller (name of the AD server), such as server2012.
3. Enter Domain name (DNS/Realm)
4. Enter the NetBIOS name.
   In the Organizational unit field, you can enter a smaller organizational unit under a large AD architecture to minimize the complexity of the configuration; e.g., Asia/China/Shanghai.
   OU: A particularly useful type of directory object contained within domains is the organizational unit. Organizational units are Active Directory containers into which you can place users, groups, computers, and other organizational units. An organizational unit cannot contain objects from other domains.

   OU: An organizational unit is the smallest scope or unit to which you can assign Group Policy settings or delegate administrative authority. Using organizational units, you can create containers within a domain that represent the hierarchical, logical structures within your organization. You can then manage the configuration and use of accounts and resources based on your organizational model. For more information about Group Policy settings, see Group Policy (pre-GPMC).
5. Enter the AD administrator's name.
6. Enter the password.
7. Enter the password again to confirm.
8. Click the Apply button. The server should take several minutes to acquire accounts from the AD server.

If preferred, click the checkbox below to remove existing Domain user and UID mapping.

If the NAS server is not present yet in an AD server's database. You can visit Active Directory Users and Computers.

Make sure to provide the users of the newly added computer (the NAS server) with full control over it.

Home Directory:

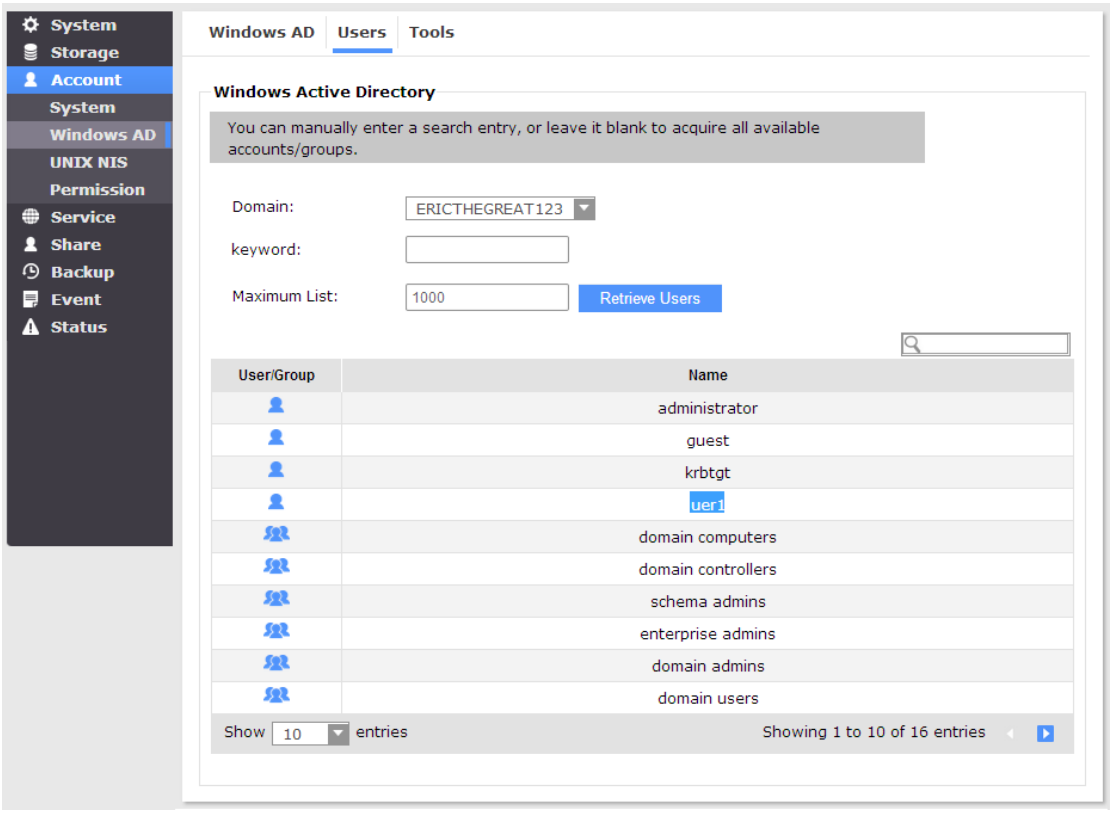
This designate the home directory for use with Windows domain users.
1. Select a location from the directory window.
2. Select Append Domain Name, if preferred.
3. Select Append User Name, if preferred.
4. Click the Apply button.

File directory similar to the organizational hierarchy tree in Windows AD will then be created in the volume you designated.

Users

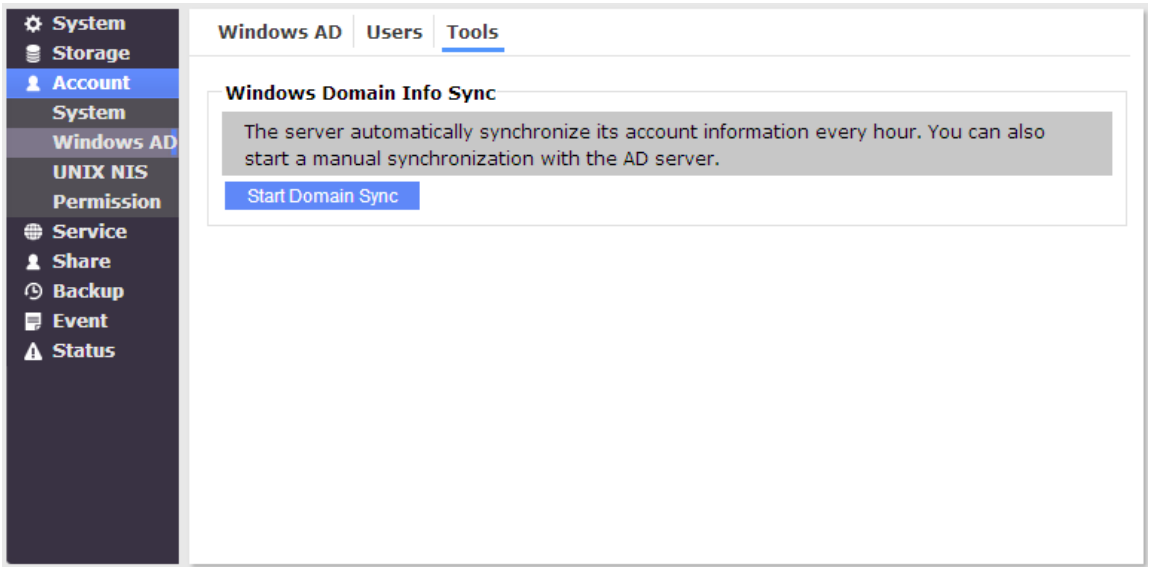
When successfully joined to an AD network, the User/Group will be listed in the **Users** page. The administrator, guest, users, and user groups will be listed. you can select a Domain from its pull-down list if you joined multiple. You can also narrow down the list by entering a Keyword, by entering a user name, and click the **Retrieve Users** button.

If there is an extremely large number of entries in the AD user/group pool, you can specify the maximum number to be listed in this window.



Tools

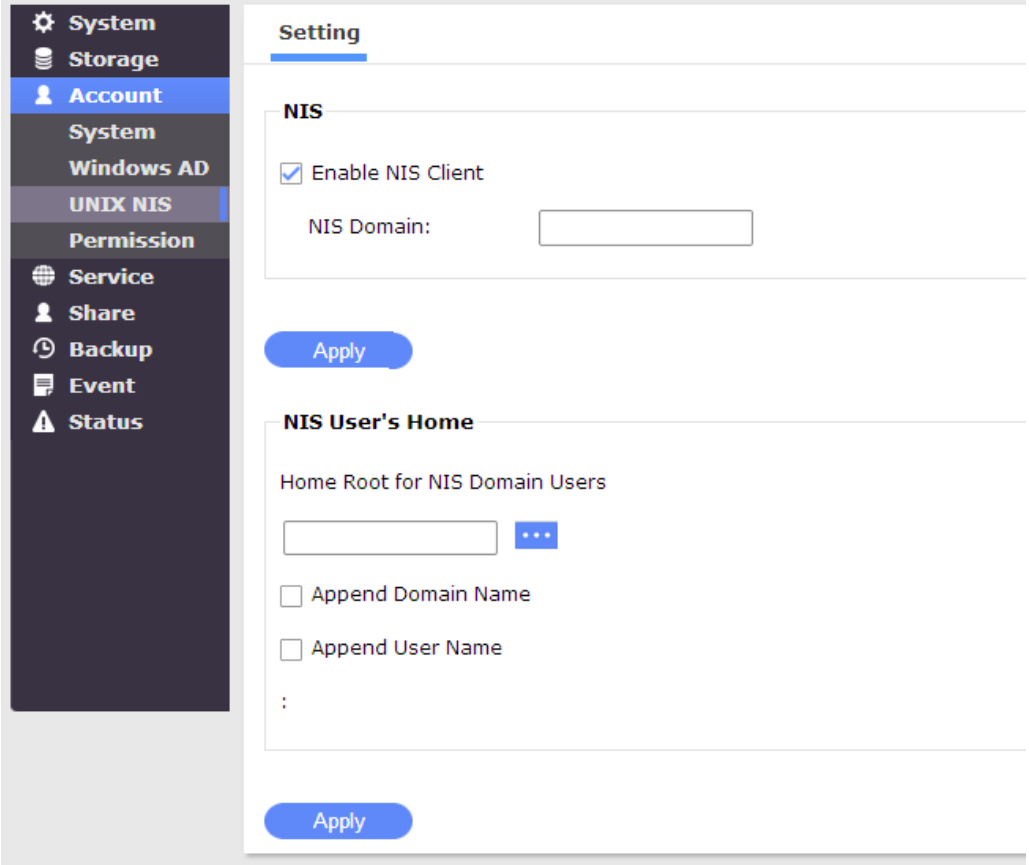
The server automatically synchronize with the AD server for its domain information by every 1 hour. You can also click the Start Domain Sync button to manually initiate an immediate synchronization process.



5.3. Account > UNIX NIS

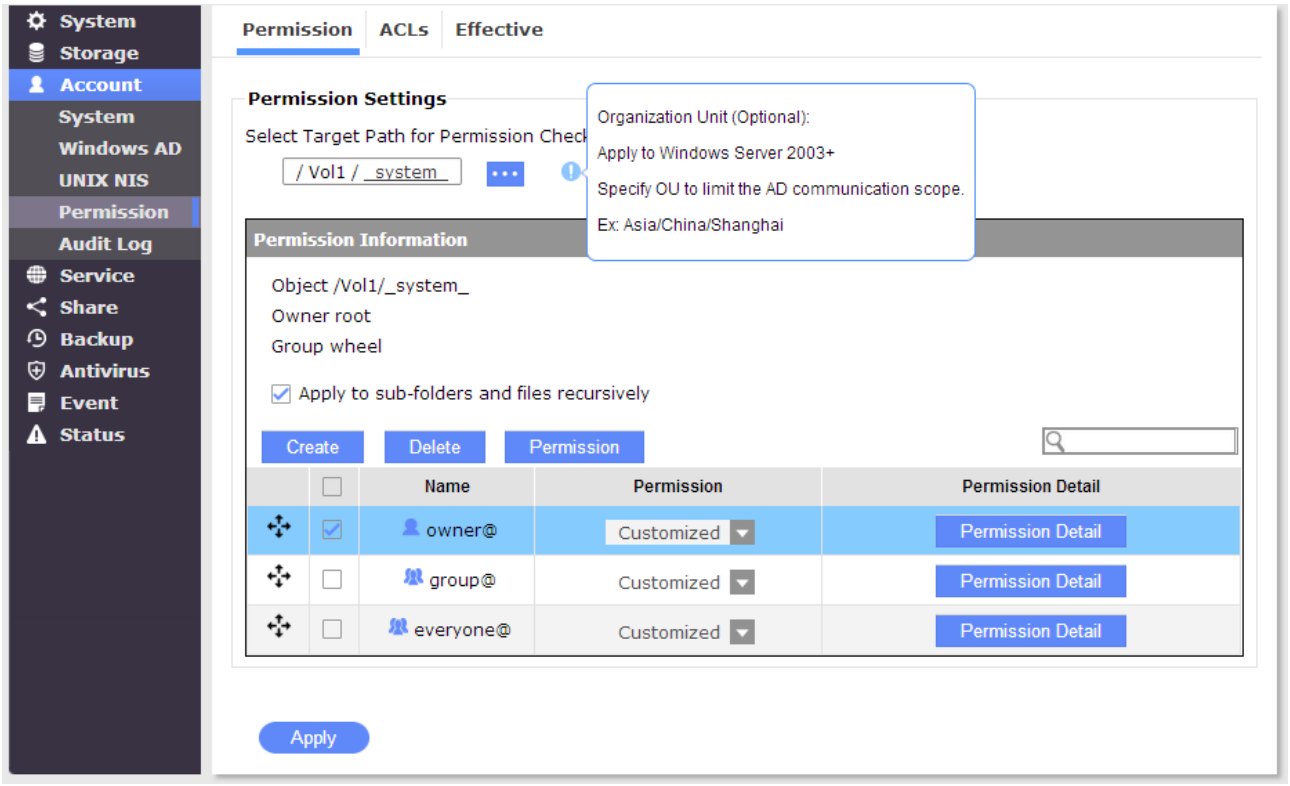
NIS (Network Information Services), previously known as Yellow Pages, is communication protocol for UNIX systems, which enables data sharing that is centrally managed. The NAS server can manage NFS cient's mount privileges and allow for UNIX/Linux computers granted by the administrator. The NAS server can acquire user account, UID/GID from an NIS server. If a UNIX/Linux computer can gain access to a share in the NAS server, users of the UNIX/Linux computer can access the share.

To join a NIS domain,
1. Click on Enable NIS client.
2. Enter the NIS Domain Name.
3. Click Apply.
4. Select a Home Root position for the NIS Domain users.
5. Select to apply Domain Name and User Name if preferred.
6. Click the Apply button.



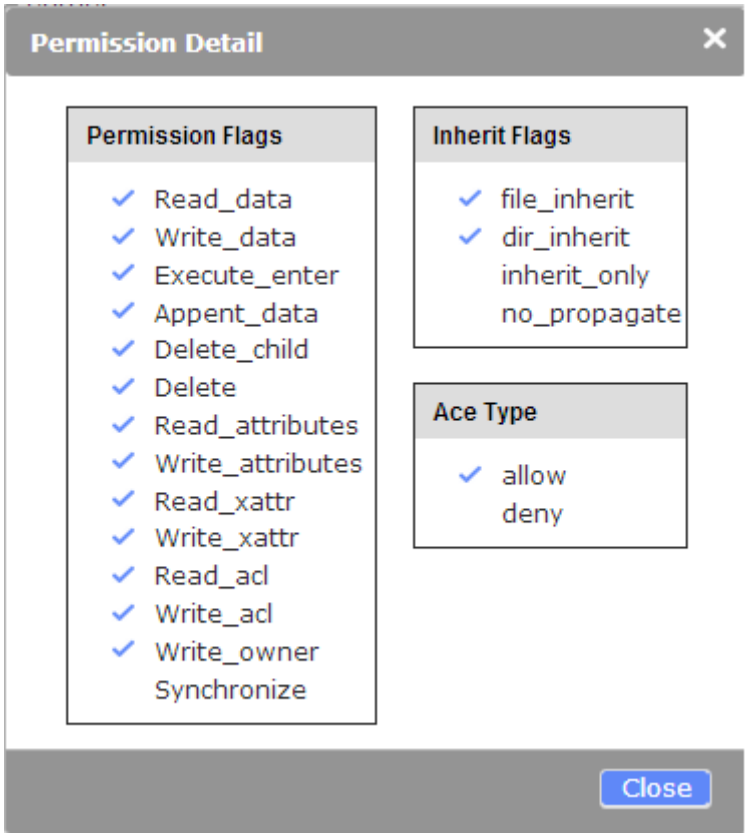
5.4. Account > Permission

You can share a specific Folder Group in a volume created in this server with others on the network. When you create a share, assign the permission to a share with the allowed or denied permission.

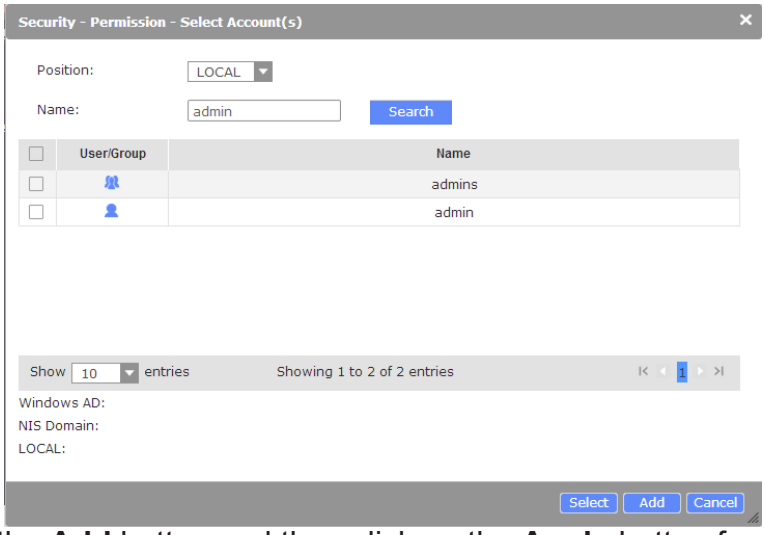


To specify a permission setting for a particular Folder Group:

1. Click on the Target Path button to determine the access permission to a target.
2. If you want to share an existing Folder Group under a volume, click the folder target name until you reach the desired directory path.
3. Click the **Create** button to display the **Add account**, **Owner permission**, **Group permission**, **Everyone**, or **permission** options.



4. Select the **Position** menu (if you have joined both Windows AD domain and having a range of local accounts). You can then enter a created name for **Search**.

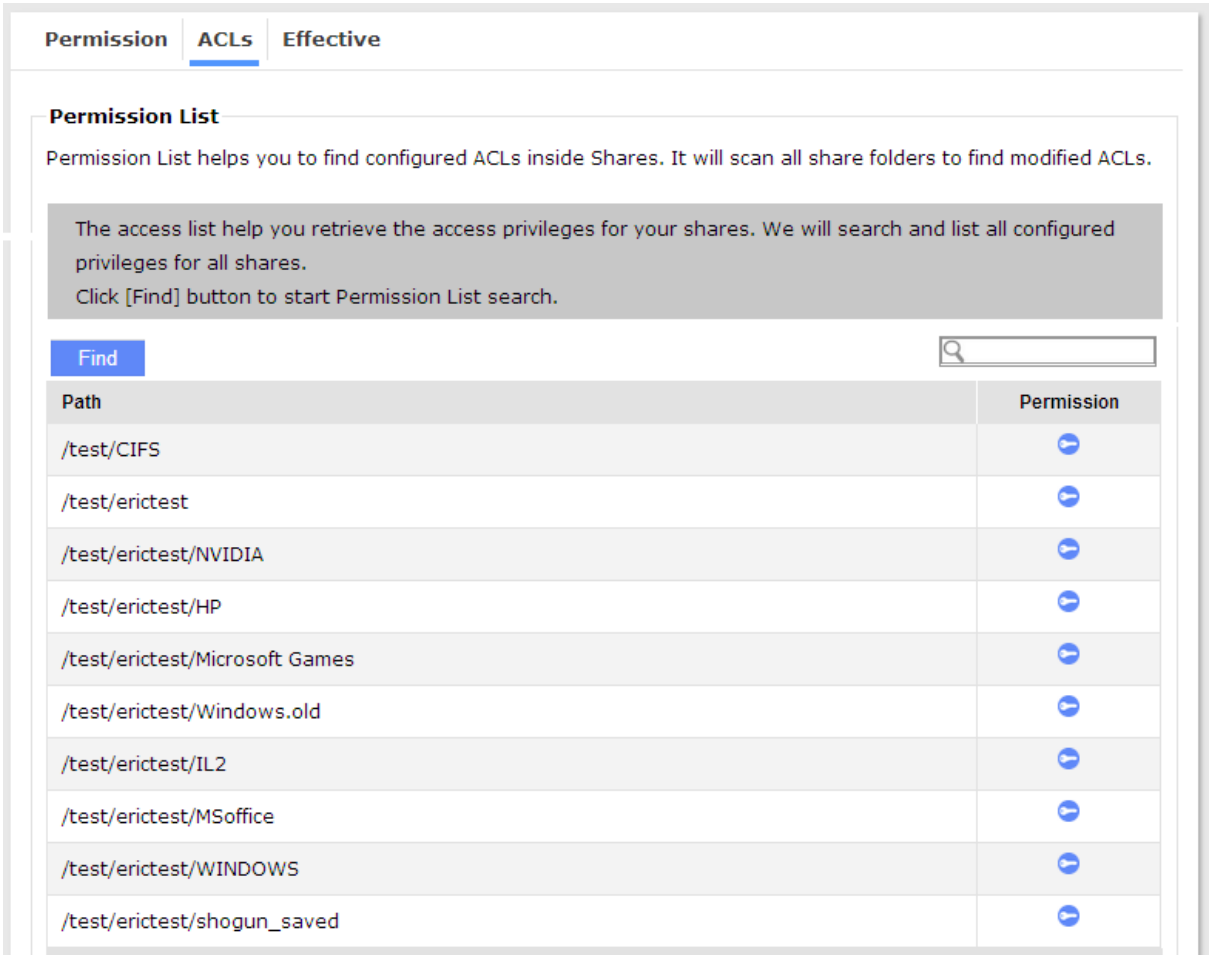


5. Click the **Add** button and then click on the **Apply** button for changes to take effect.

5.5. Account > Permission > ACLs

The main function of this window is to list the folder for which the ACL feature has been configured. If the default privileges have not be altered, the Folder Groups will not be displayed. If the ACL attributes have been configured, only two directory levels will be displayed.

Access Control Lists (**ACL**) are associated with files and folders, and the list of users and groups which are allowed to access the files or folders. When a user is granted access to files or folders, an ACL node is generated and an account is created for that file or folder. Whenever you create a permission to a user, a Security ID (SID) is created by the NAS server, and it will be referred to by the ACL for security concerns. If changes are to be made to the user, the SID will remain, and hence the administrator will have to configure the group member relationships and access rights.



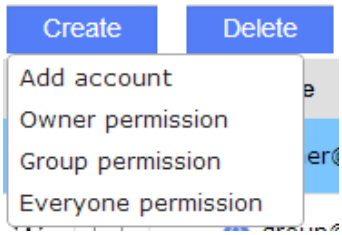
Admin and Guest within group accounts **Admins** and **Everyone** are built-in accounts.

Every user of the NAS server (local, Domain, and NIS users) belong to the **Everyone** group. When a volume is created, Admins, Admin, and Everyone will be granted the full control access rights. Any files or folders created under the volume will inherit the same access rights.

Users and groups managed by Local, Windows AD, and NIS servers are supported.

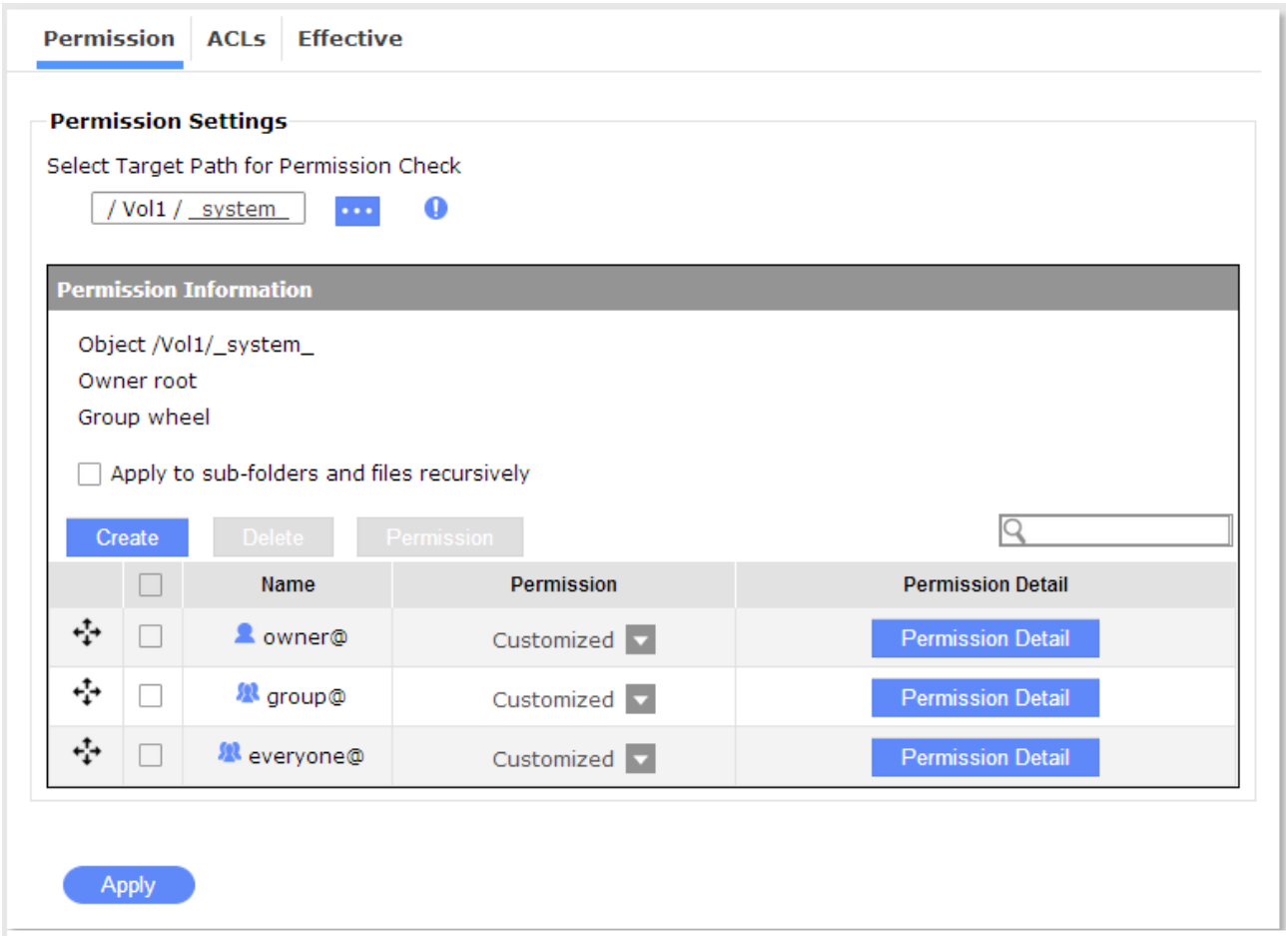
Regardless of how you access a data share via FTP, SMB, or AFP protocol, the access privileges will be determined by the ACL privilege settings here.

To change a permission for a Folder Group or group:
1. In the Permission Settings column, select the Target Path using the Location window.
2. When the Permission Information window appears, check the current permission list.
3. On the occasion that you need to create or delete User or Group permission, click on the Create button.



4. you can assign the following File/Folder permission to a user.

No Action (NA) - Account is denied from the access.
Read Only (RO) - Account is allowed to read the file or Folder Group.
Read Write (RW) - Account is allowed to read and write to the file or Folder Group, and allowed to delete it.
FC - Account allowed for Full Control.

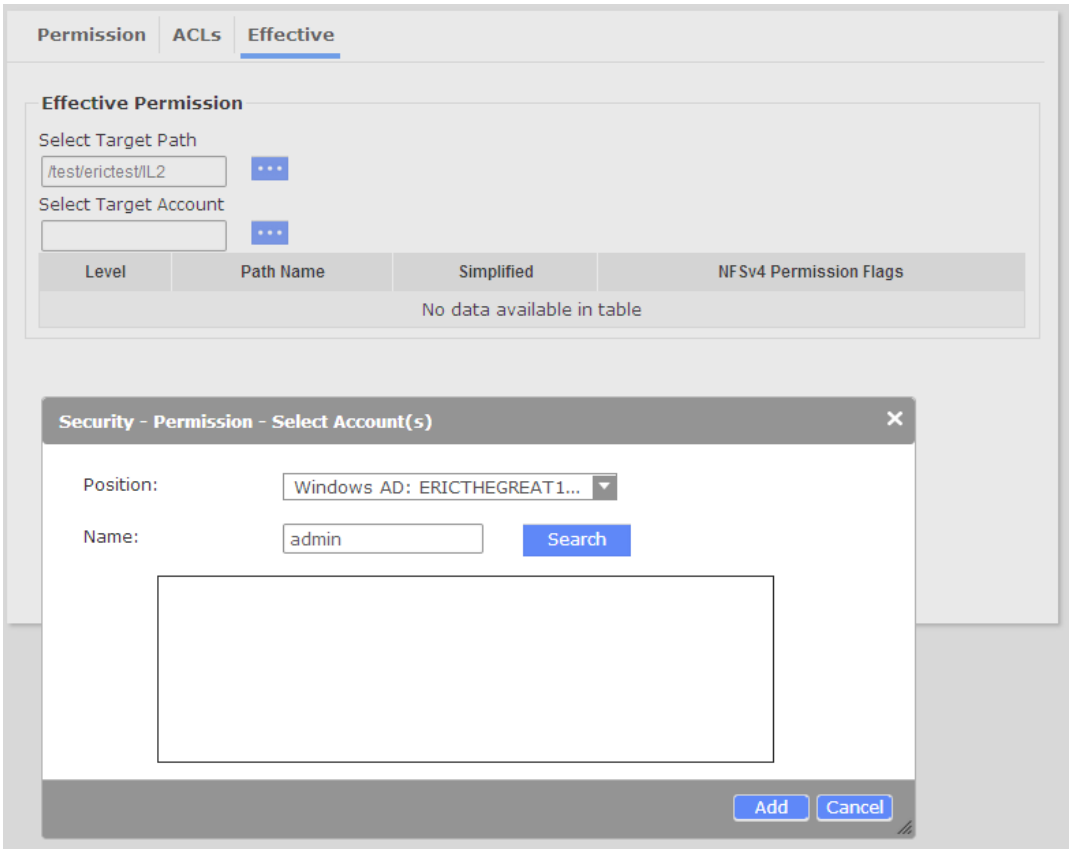


5.6. Account > Permission > Effective

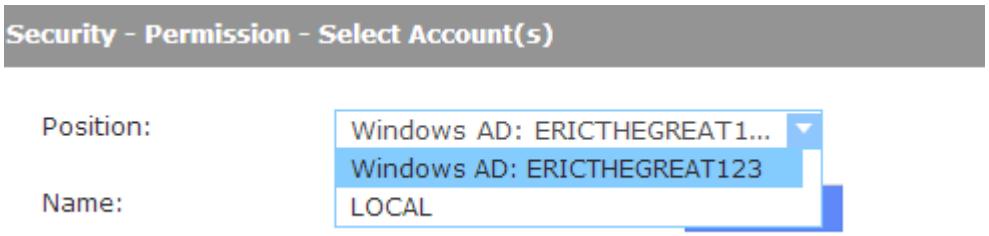
This window provides access to the list of effective permissions for particular target path. The target path points to a shared Folder Group within the volume.

To check the effective permission,

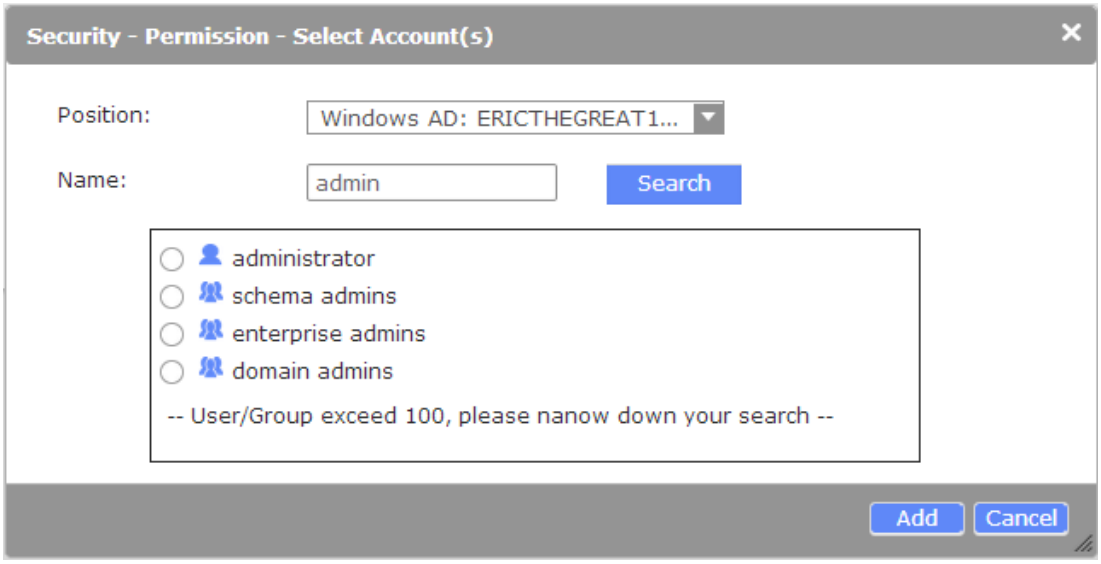
1. First select a target path from the Directory Find button ... .
2. Select a Target Account using the Find button ... .



3. The **Select Account(s)** window will appear. Select a Position (for example, either a Windows domain or Local user account).



4. You can then enter a name in the Search entry, and then click **Search**. The accounts having effective access rights to the path will be listed.
   You then select a user group to narrow down a search. Click Add to display the list of target path the account can access.



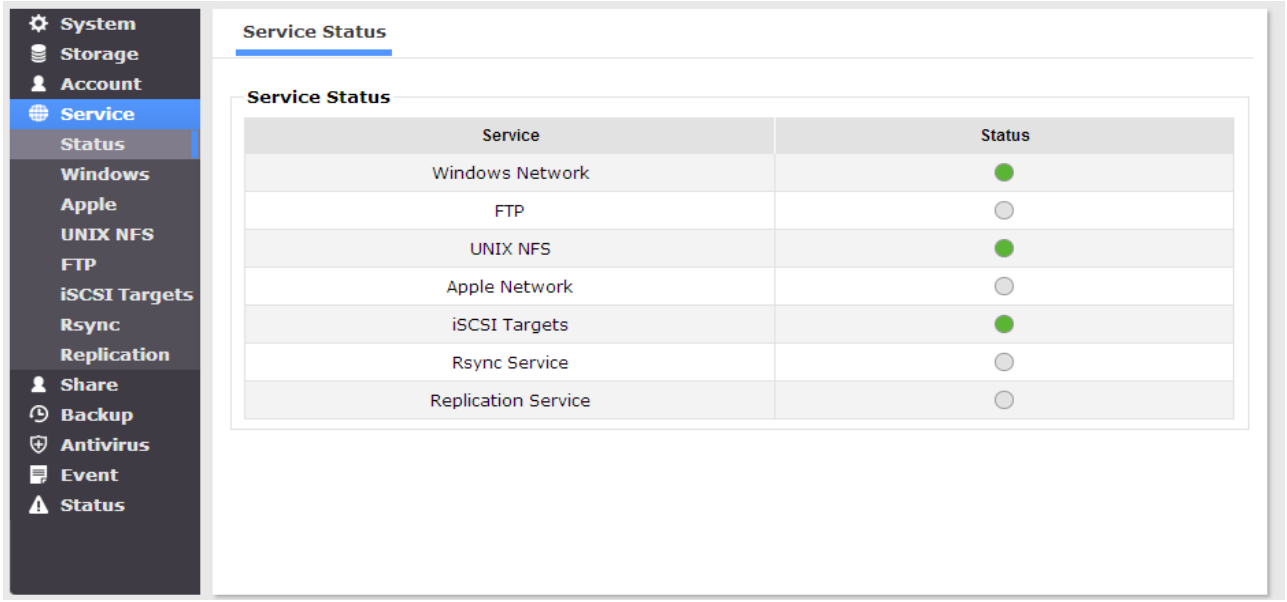
Chapter 6 Service

The Service windows provides access to the sharing protocols in Status, Windows, Apple, UNIX NFS, FTP, iSCSI Targets, Rsync, and Replication.

6.1. Service > Status

The Service > Status page provides access to the sharing conditions of all shares to different file systems over different protocols, iSCSI Targets, and system data Rsync and Replication configurations. The services currently enabled and running will be indicated by a green light.

If any of the service is not enable, click on the unlit circle to move to its configuration page.



6.2. Service > Windows

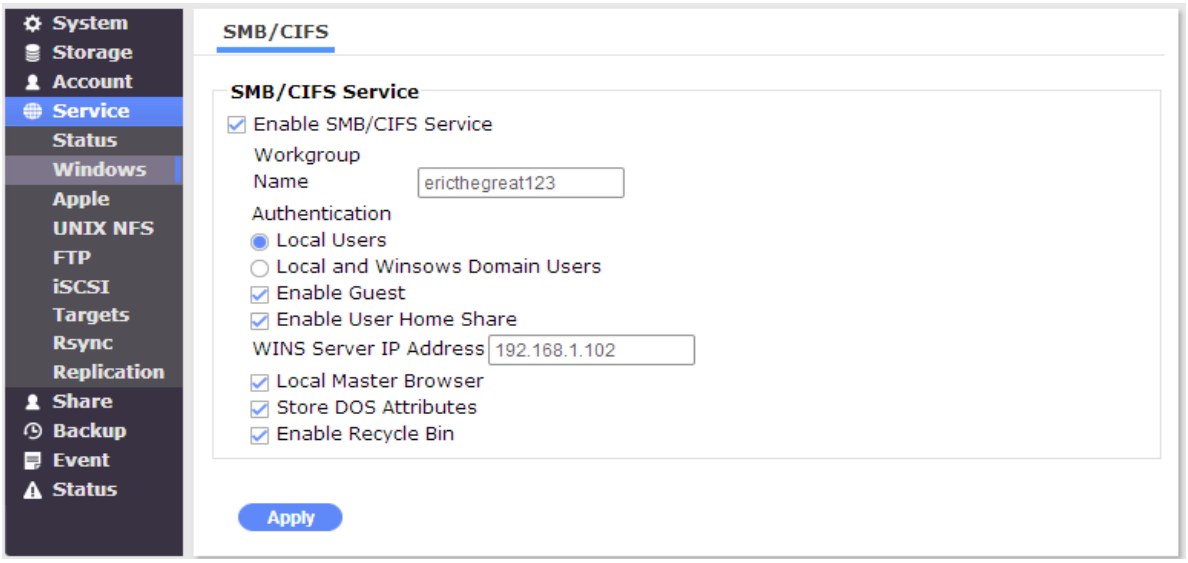
The NAS server utilizes SMB/CIFS protocol (Server Message Block/Common Internet File System), a protocol used by Microsoft to share files, directories, and devices with the Windows client.

Note the following with the workgroup mode and the domain mode:

1. You select the **Local Users** checkbox to enable the **workgroup mode**.
2. When you join a Windows AD domain in the **Account** > **Windows AD** window, the SMB/CIFS service is automatically started. By then, the SMB/CIFS service is automatically configured to the domain mode and enabled.

The NAS server becomes a member of a workgroup and communicates with the clients using the configured database for access authentication. In this way, other authentication server in the network is not required.

With a **Domain mode**, the NAS server listens to a domain controller and communicates with clients using the database stored on server. You should register the NAS server to the domain. Kerberos will be applied as the authentication service.



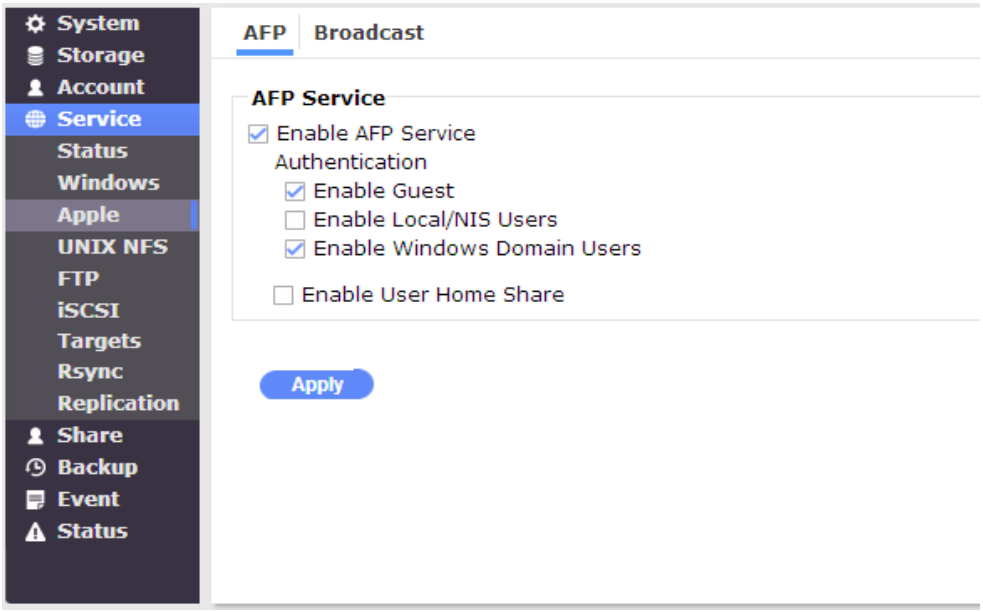
6.3. Service > Apple

You can enable Mac file service to let the NAS server manage a Mac file server (AFP Server).

The NAS server supports two kinds of protocols used for Mac OS clients –TCP/IP (Open Transport) and Both AppleTalk and TCP/IP. Also, NAS server provides two kinds of security polices for Macintosh Network AFP client.
Local account and NIS authentication: Authenticate user using NAS server's internal user database.
Local and domain authentication: If Windows Network is enabled, you can enable both local and domain authentication for AFP client.

Enable Guest: Check to enable the guest login.
Configuring Macintosh network settings

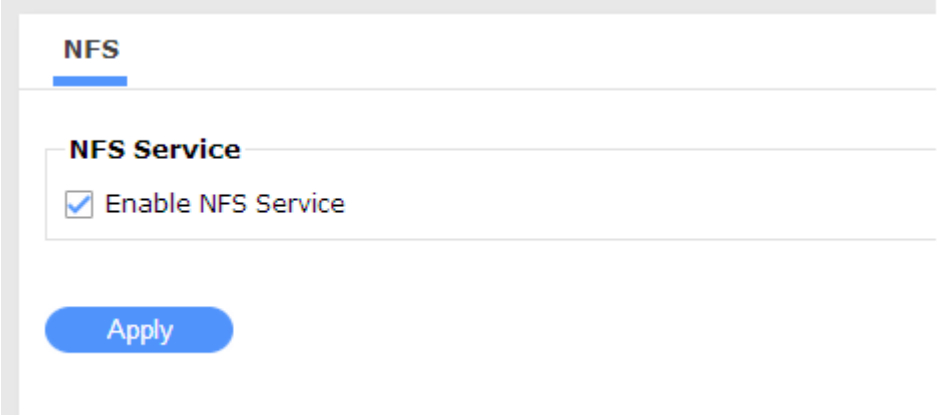
1. Click the **Enable Macintosh Network** (**AFP Protocol**) checkbox to enable access for AFP client.
2. Click the Local account authentication/NIS checkbox to authenticate user using the server's local user database.
3. Or, click the Domain account authentication checkbox to use both local account and Microsoft domain security authentication.
4. Click Apply to save the setting.



6.4. Service > Unix NFS

Click the **Enable UNIX/Linux Network** (NFS Protocol) checkbox to enable access for NFS clients.

Click **Apply** to save the settings.



6.5. Service > FTP

The NAS server supports File Transfer Protocol (FTP) that allows users to transfer files via the Internet.

Configuring FTP data access

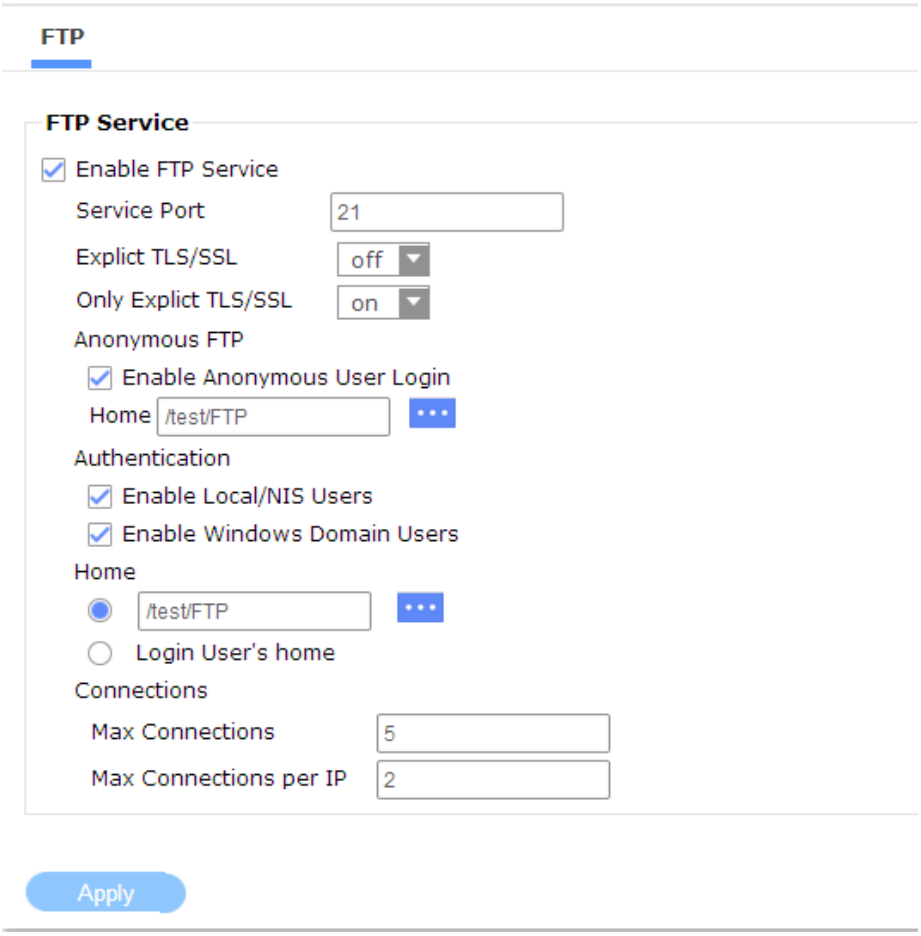
1. Click Enable FTP Service checkbox to enable all of the configurable options.

2. Select a suitable FTP port. Usually the FTP port #21 is needless to change.

3. Only Explicit SSL/TLS: Enable this option to encrypt data transfers when the FTP clients login with SSL/TLS mode to access data that will enforce the transferred data with more security. For example: Using FileZilla as the FTP clients and select “Require explicit FTP over TLS.”

Enable Anonymous User login: Enable this option for let anonymous login and map to local account for the access rights to someone who is already in the NAS server’s user database.

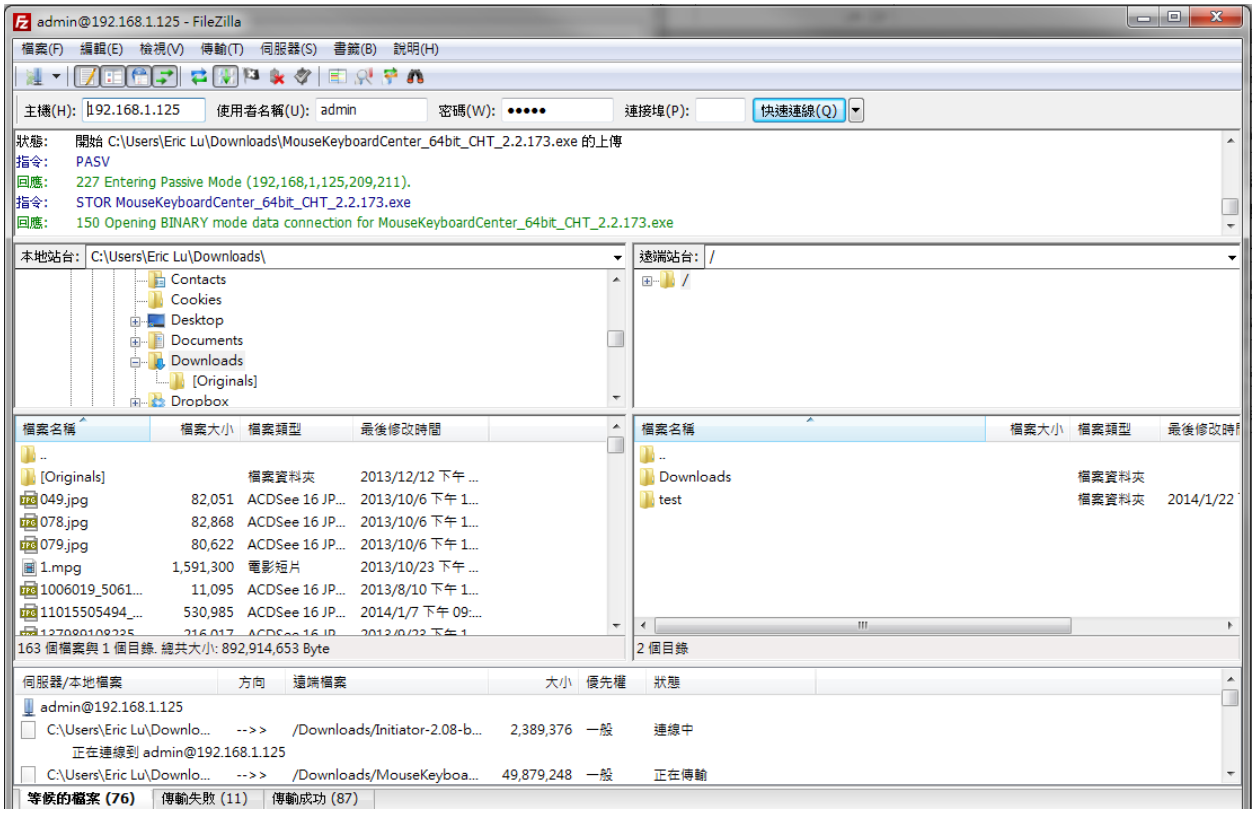
Local/NIS users: for users that have already been certified by the NAS server.
Windows Domain Users: for users that have been imported from a Windows Domain.
Home: you can use the search button on the right to search for a local file directory position where will be the FTP server's default home directory (once it is accessed via the FTP protocol.



Login User's home: if selected, once a user logs in to the FTP server, he/she will enter the designated Folder Group or directory that was specified for his/her access.

Connections: Use the number entries to specify how many connections are allowed simultaneously.

You can then use an FTP client software, enter the NAS server's IP address, user name, and password to upload or download files to/from the FTP Folder Group.


admin@192.168.1.125 - FileZilla
檔案(F) 編輯(E) 檢視(V) 傳輸(T) 伺服器(S) 書籤(B) 說明(H)
主機(H): 192.168.1.125 使用者名稱(U): admin 密碼(W): ••••• 連接埠(P): 快速連線(Q)
狀態: 開始 C:\Users\Eric Lu\Downloads\MouseKeyboardCenter_64bit_CHT_2.2.173.exe 的上傳
指令: PASV
回應: 227 Entering Passive Mode (192,168,1,125,209,211).
指令: STOR MouseKeyboardCenter_64bit_CHT_2.2.173.exe
回應: 150 Opening BINARY mode data connection for MouseKeyboardCenter_64bit_CHT_2.2.173.exe
本地站台: C:\Users\Eric Lu\Downloads\
Contacts
Cookies
Desktop
Documents
Downloads
[Originals]
Dropbox
遠端站台: /
檔案名稱 檔案大小 檔案類型 最後修改時間
[Originals] 檔案資料夾 2013/12/12 下午 ...
049.jpg 82,051 ACDSee 16 JP... 2013/10/6 下午 1...
078.jpg 82,868 ACDSee 16 JP... 2013/10/6 下午 1...
079.jpg 80,622 ACDSee 16 JP... 2013/10/6 下午 1...
1.mpg 1,591,300 電影短片 2013/10/23 下午 ...
1006019_5061... 11,095 ACDSee 16 JP... 2013/8/10 下午 1...
11015505494_... 530,985 ACDSee 16 JP... 2014/1/7 下午 09:...
163 個檔案與 1 個目錄. 總共大小: 892,914,653 Byte
Downloads 檔案資料夾
test 檔案資料夾 2014/1/22
2 個目錄
伺服器/本地檔案 方向 遠端檔案 大小 優先權 狀態
admin@192.168.1.125
C:\Users\Eric Lu\Downlo... --->> /Downloads/Initiator-2.08-b... 2,389,376 一般 連線中
正在連線到 admin@192.168.1.125
C:\Users\Eric Lu\Downlo... --->> /Downloads/MouseKeyboa... 49,879,248 一般 正在傳輸
等候的檔案 (76) 傳輸失敗 (11) 傳輸成功 (87)

6.6. Service > iSCSI Targets

The iSCSI Target panel present storage shares known as Logical Disks as iSCSI targets to the computer equipped with hardware or software iSCSI initiators.

The NAS server's iSCSI storage supports iSCSI initiators that comply with the IETF iSCSI standard (RFC 3720). The configuration efforts should include the following:

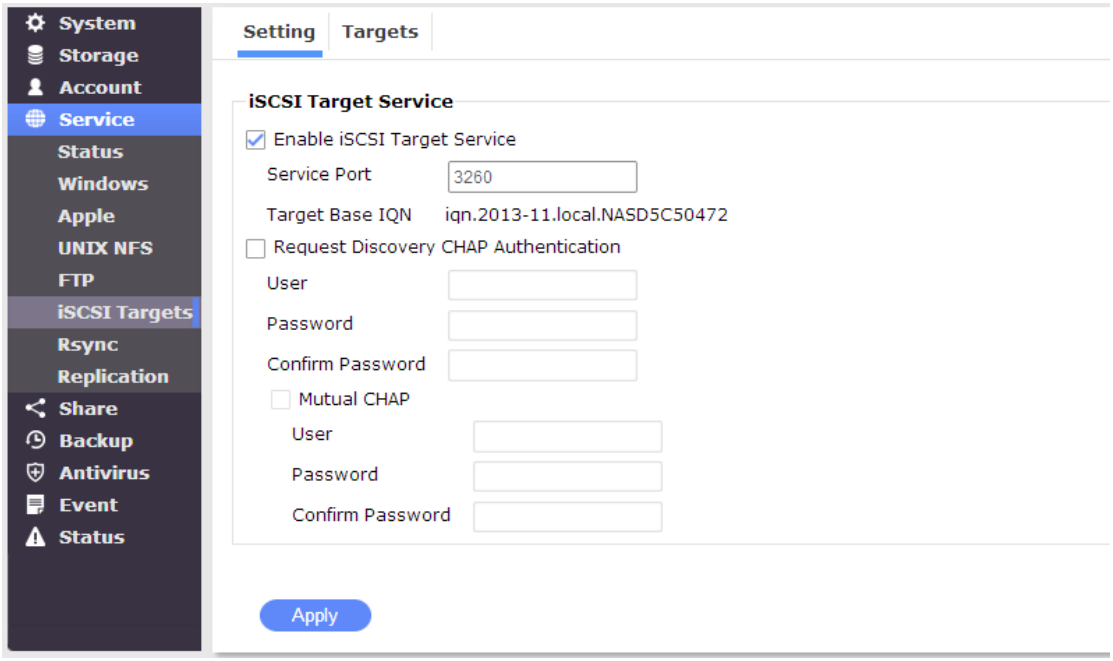
1. Configuring host port IPs and connectivity settings.
2. Setting CHAP and other authentication options.
3. Making network shares volumes available through the Gigabyte Ethernet host ports.

See page 95 for how to create a Logical Disk.

IMPORTANT:

Before you can share a portion of the system volume as an iSCSI target, please create a Logical Disk in Storage > Logical Disks.

To enable an iSCSI target over the network, select the **Enable iSCSI Target Service** checkbox. The default service port **3260** and **Target Base IQN** will automatically be generated, depending on the current domain and server name you currently possess. For security reasons, see the CHAP and the configuration options in the Targets tabbed menu.

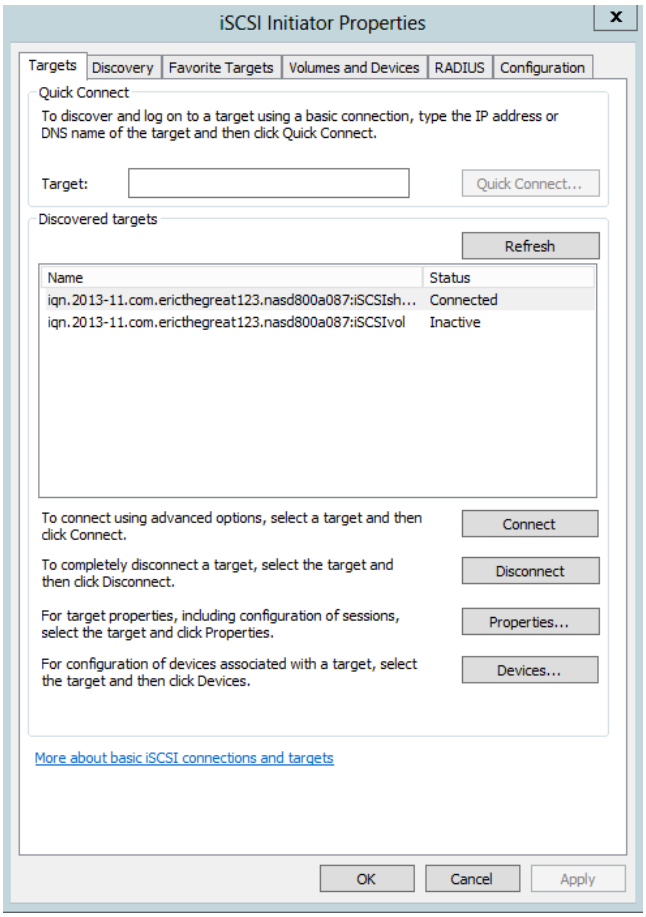


To start the iSCSI initiator, go to **Control Panel** > **System and Security** > **Administrative Tools**.

The alternative to run the iSCSI Initiator through that path is to execute it by name.
All you need to run is iscsicpl.exe.

You can go to Start and in the blank,
enter "**iscsicpl.exe**."

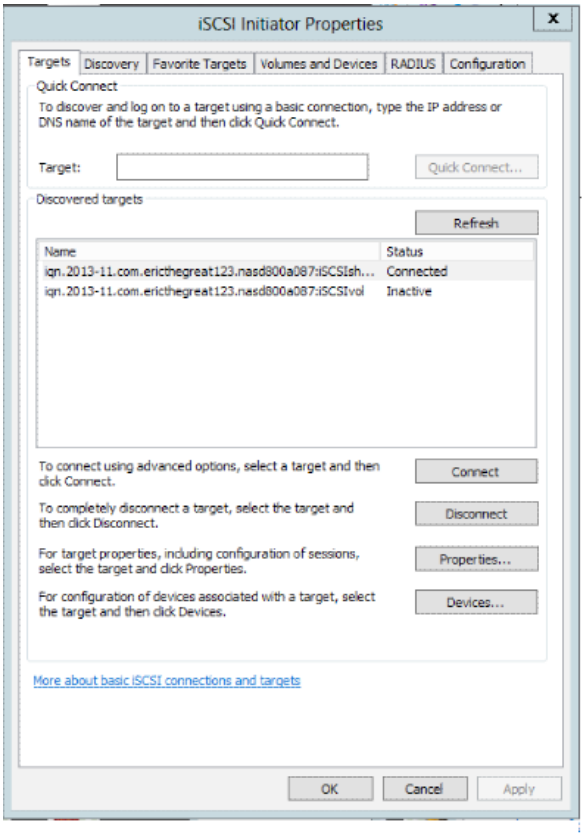
From the initiator,
Enter the NAS server's IP address in the Target's entry, then click the **Quick Connect...** button.

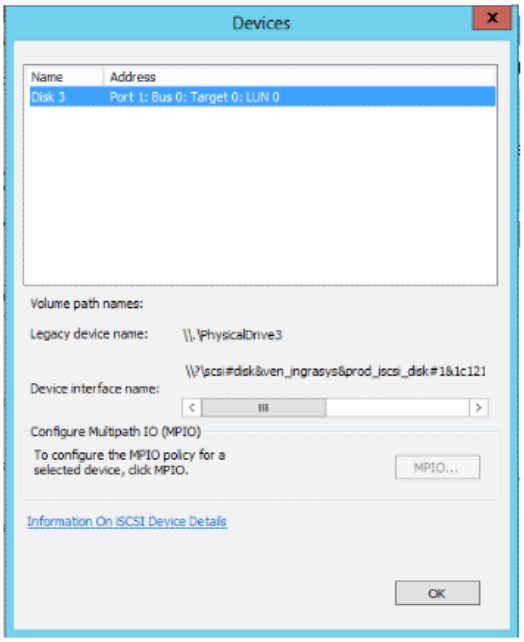


The iSCSI's IQN name should be listed in the Discovered targets below. If it is not shown, please check your network configuration.

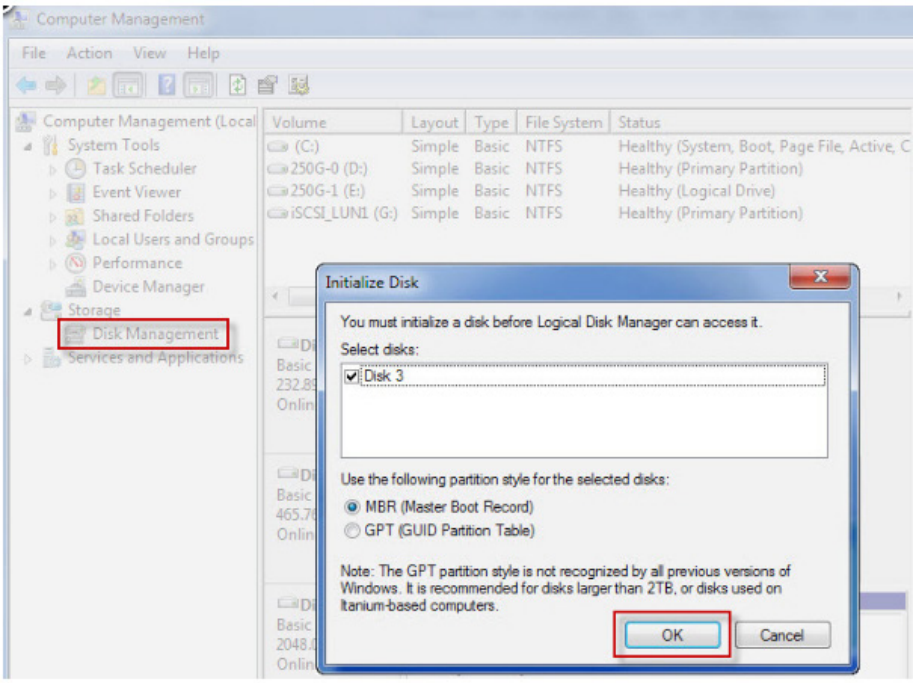
When the iSCSI target's IQN (that configured on the NAS server) is shown, click on the **Connect** button. The Devices (iSCSI target) shown as Disk # should be displayed as "Disk# Port#: Bus # Target#: LUN #".

Click **OK** to proceed.

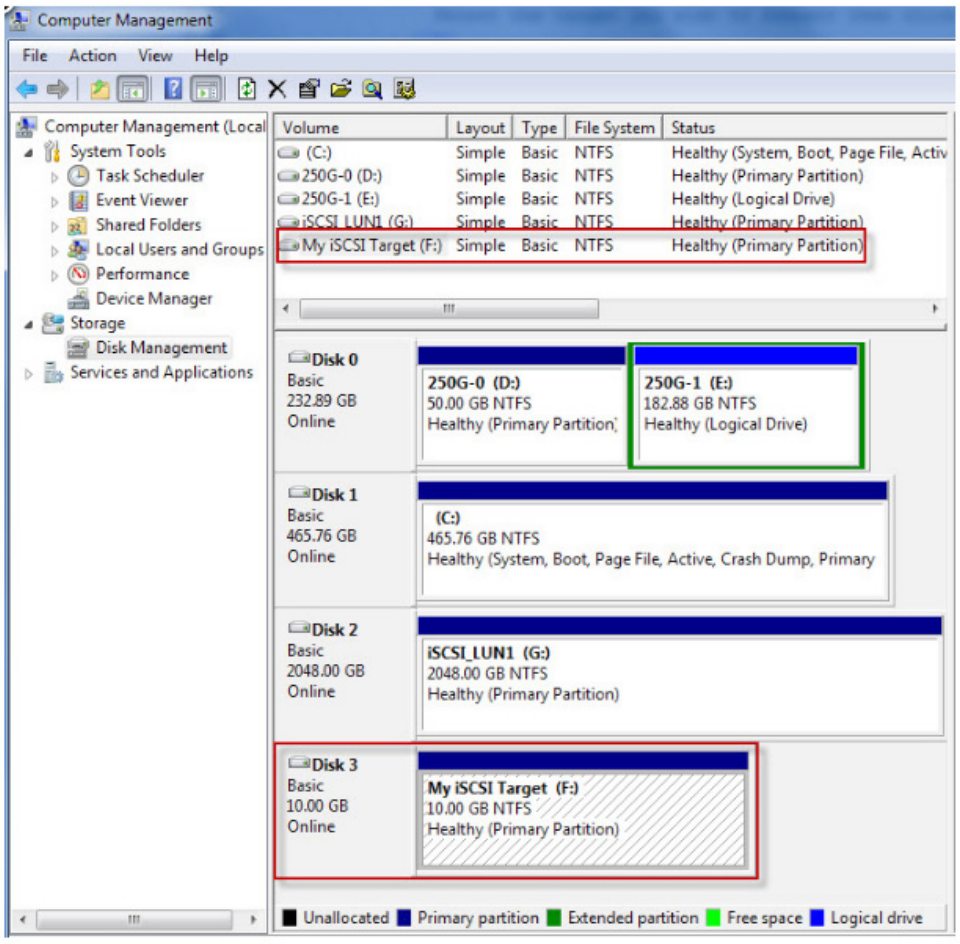




Go to Computer Management. Click on **Storage** > **Disk Management**. An iSCSI target will appear as an un-initialized disk volume. Right-click to initialize the target volume.


Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Volume Layout Type File System Status
(C:) Simple Basic NTFS Healthy (System, Boot, Page File, Active, C
250G-0 (D:) Simple Basic NTFS Healthy (Primary Partition)
250G-1 (E:) Simple Basic NTFS Healthy (Logical Drive)
iSCSI_LUN1 (G:) Simple Basic NTFS Healthy (Primary Partition)
Initialize Disk
You must initialize a disk before Logical Disk Manager can access it.
Select disks:
Disk 3
Use the following partition style for the selected disks:
MBR (Master Boot Record)
GPT (GUID Partition Table)
Note: The GPT partition style is not recognized by all previous versions of Windows. It is recommended for disks larger than 2TB, or disks used on Itanium-based computers.
OK
Cancel

When done, the iSCSI target can be used as one of your storage devices.

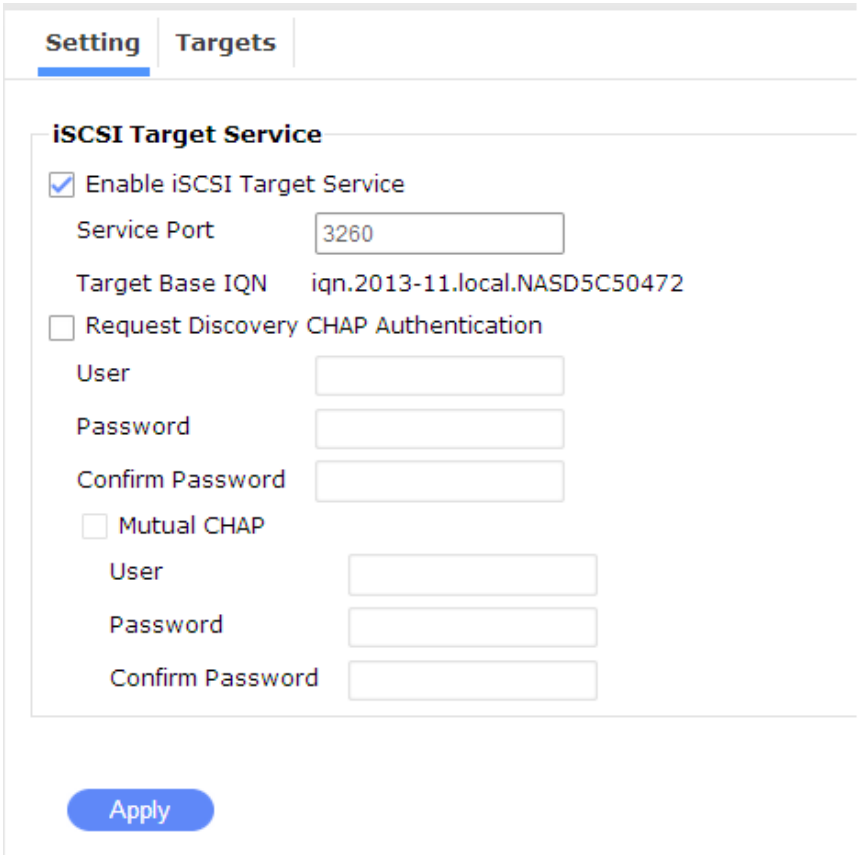


Using CHAP Authentication

CHAP stands for Challenge Handshake Authentication protocol. With this protocol, networked computers use the encrypted password to authenticate each other remotely. The CHAP security method can be used to build a secure iSCSI network.

The server supports one-way or two-way (mutual) CHAP authentication. With two-way CHAP, a separate three-way handshake is initiated between an iSCSI initiator and storage host port. The initiator side (for example, Microsoft initiator software), CHAP logon is designated as an option with selectable initiator IQN name and that of the target secret (to which the CHAP authentication call will be issued; namely, the host port on your server).

To enable the CHAP authentication, select the "**Request Discovery CHAP Authentication**" checkbox to activate the feature.

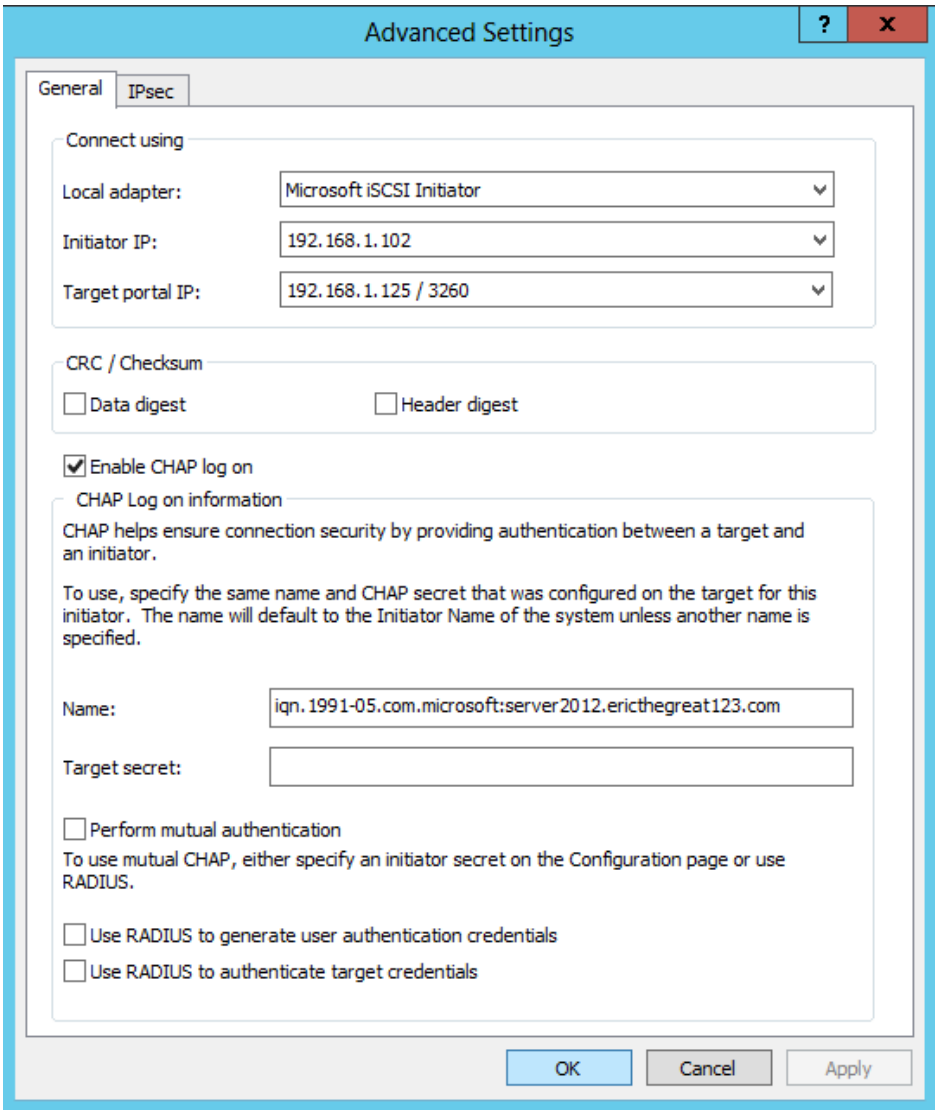


The user name here applies to the one-way or Mutual CHAP authentication. Identical names and passwords must be configured here and on the initiator software or HBA configuration utility.

User/target name and password are used for the inbound authentication processes between the called and calling parties. Names and passwords are identical here and on the initiator side.
User name should contain at least 12 characters.

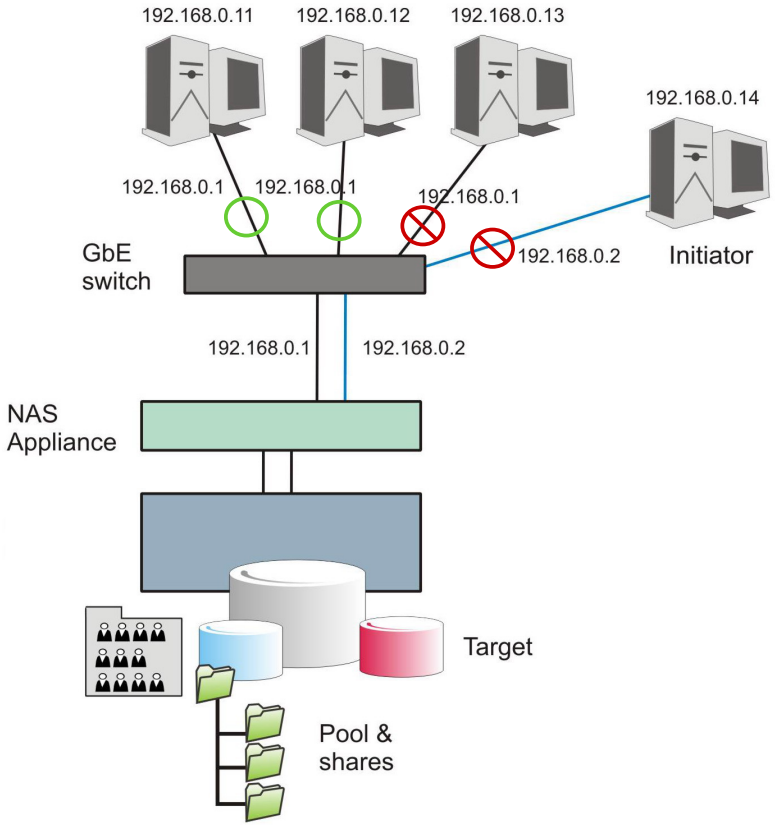
The user password here applies to a one-way CHAP configuration for inbound authentication. Note that some CHAP configuration utilities may use "secret" instead of "password."

To make the secure CHAP connection, enter the same name and password (secret) on your iSCSI initiator setting page on the host computer.

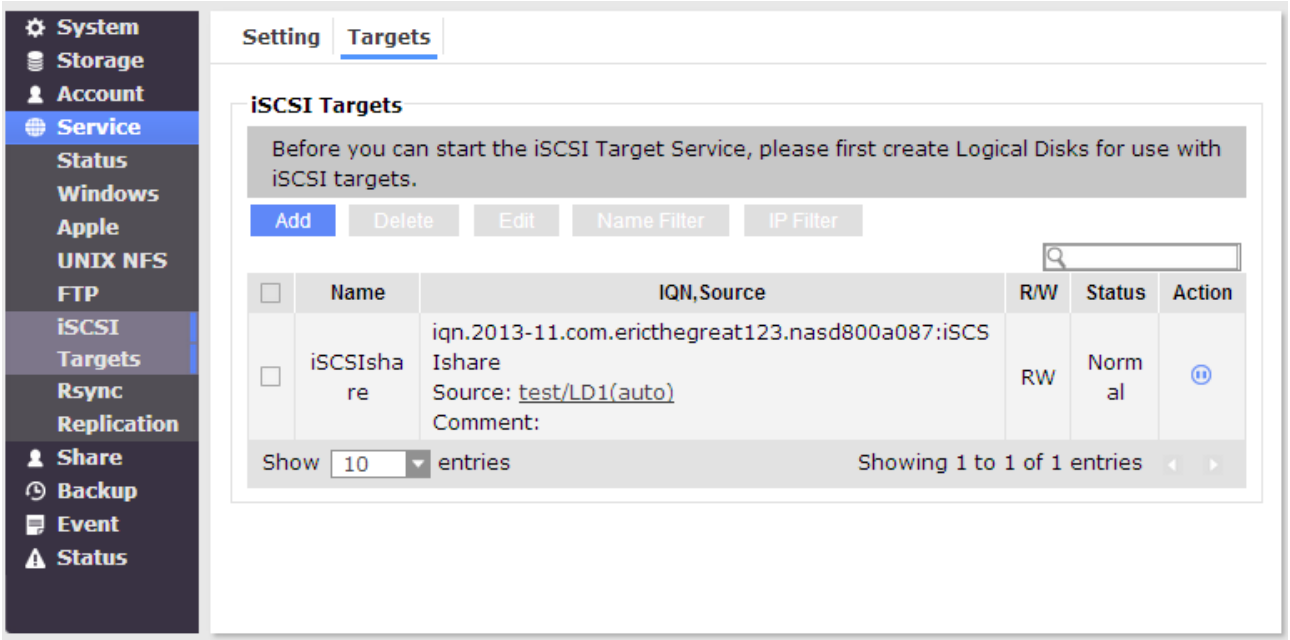

Advanced Settings
General
IPsec
Connect using
Local adapter:
Microsoft iSCSI Initiator
Initiator IP:
192.168.1.102
Target portal IP:
192.168.1.125 / 3260
CRC / Checksum
Data digest
Header digest
Enable CHAP log on
CHAP Log on information
CHAP helps ensure connection security by providing authentication between a target and an initiator.
To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.
Name:
iqn.1991-05.com.microsoft:server2012.ericthegreat123.com
Target secret:
Perform mutual authentication
To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.
Use RADIUS to generate user authentication credentials
Use RADIUS to authenticate target credentials
OK
Cancel
Apply

Targets

The Targets page allows you configure individual iSCSI targets and filter out computers that you do not want to have the access. In a network environment where multiple computers reside, you may exclude the access from some computers to an iSCSI target from the access list.



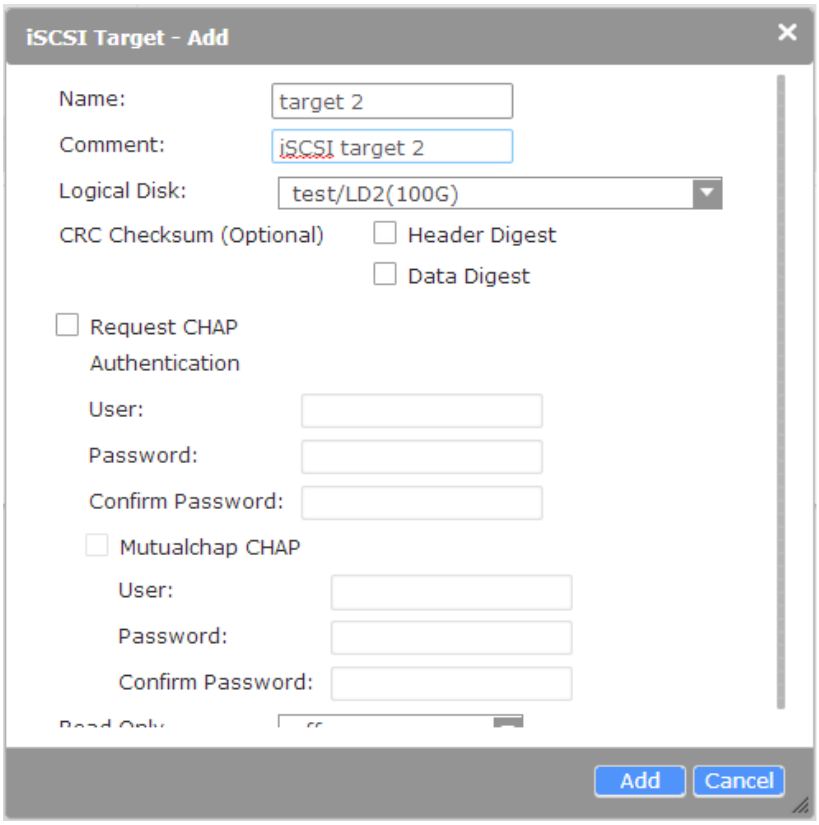
To start the configuration, click **Add** or click on an existing iSCSI target, on its checkbox.



To create a new iSCSI target, click on the Add button. The Add window will appear. Enter a name, comment, and select a Logical Disk.

NOTE:

You must create Logical Disks in the **Storage** > **Logical Disks** window before you can present an iSCSI target to the network.



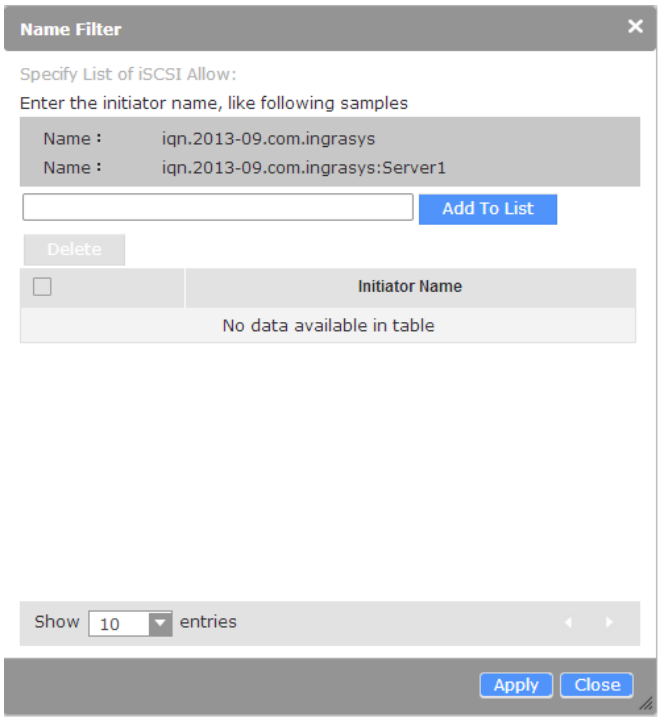
If preferred, enter the **CHAP authentication** user name and passwords. It is recommended you jot down these user names and passwords for later configurations on your host computers.

To delete an existing target, select its checkbox and click the **Delete** button.

You may change the associated attributes using the **Edit** button, such as changing the CHAP user names and passwords.

Name Filter

You may manually enter the iSCSI IQN name for the host computers that can access a specific iSCSI target. Please refer to your host computers' iSCSI initiator setting for their IQN names.



IP Filter

You may also specify the access list using the IP address, IPv6 address, or the range of subnet (using the **CIDR** format) to designate a range of computers within a local network that can access the iSCSI target.

NOTE:

If no **Name Filter** or **IP Filter** has been configured, all computers within your network can access the iSCSI target and set up a connection with it.

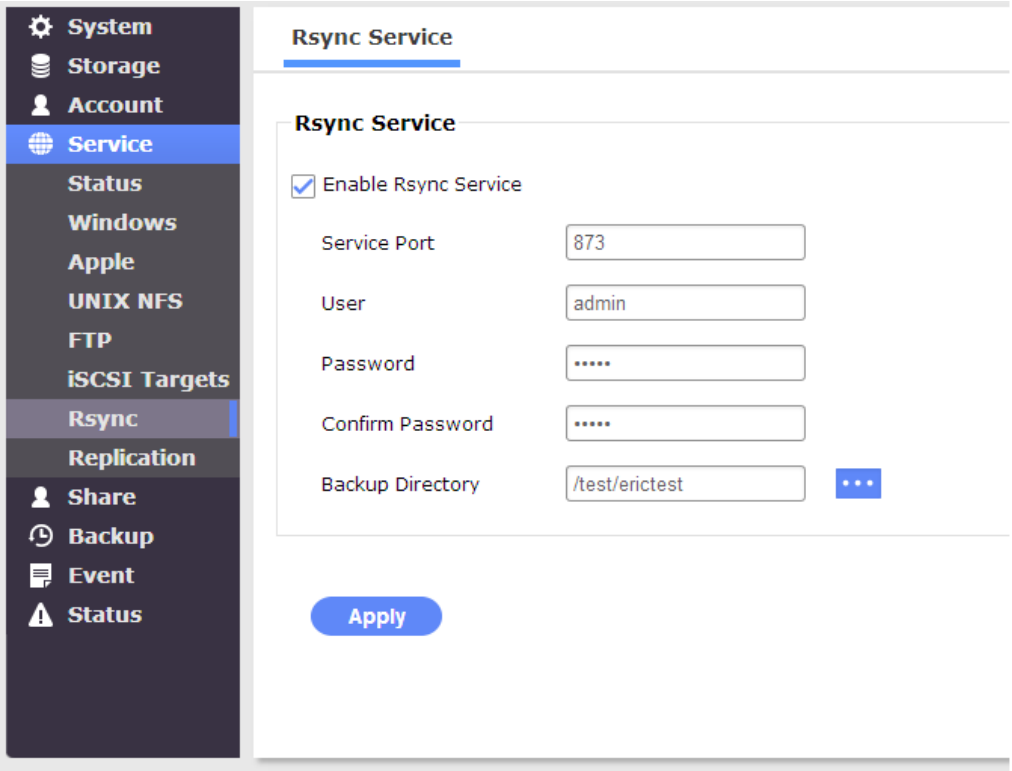
6.7. Service > Rsync

Rsync is used to keep directories on different servers in sync. The main advantage of Rsync (such as a simple copy) is that it is a efficient algorithm to copy only the files (or the part of the files) that have been changed. Using Rsync together with the Snapshot feature of this server, you can create a fast disk based backup solution with automated versioning.

IMPORTANT:

The Rsync operation requires coordination with the **Backup** > **Rsync** configuration described on page **134**. Please refer to that for complete solution.

To configure the Rsync service,



1. Select the Enable Rsync Service checkbox.
2. The Service Port, **873**, must be identical to that configured on the backup NAS server.
3. Enter a User name.
4. Enter a password and confirm the password.
5. Select a directory to be backed up as a **Backup Directory** from the selection menu.
6. Click the **Apply** button.

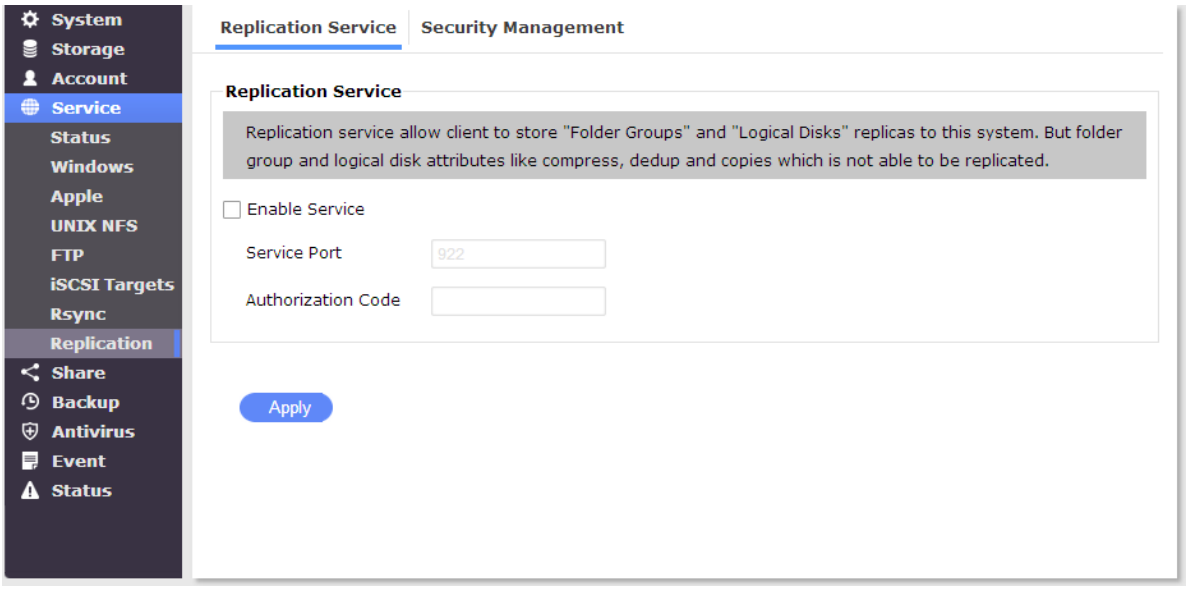
IMPORTANT:

When applying the Rsync function, the account and password are irrelevant to the system accounts. You can create new account name and password for the Rsync operation.

6.7. Service > Replication

Replication can be used as a one-time, or a regular copy from one source system to destination target on another server. It is preferred that both NAS servers must reside in the same local area network. If bandwidth is allowed, the target NAS server can reside across the Internet. You can create a fully backup of the primary storage at a specific point in time or at the specified intervals. In this way, you can create daily, monthly backup points the way as using snapshots.

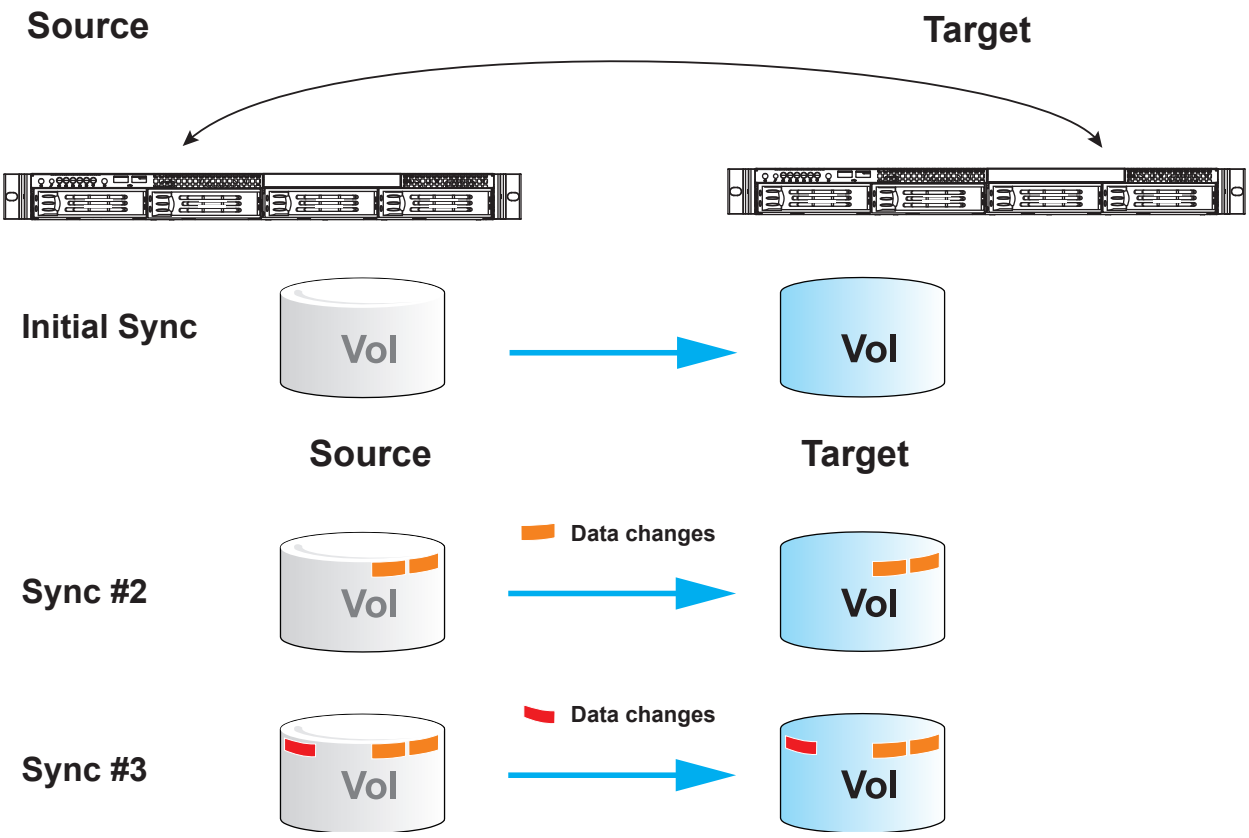
To enable the Replication service between a source and target servers, select the **Enable Service** checkbox, the default Service Port is **922**, and often unnecessary to change. Enter the **Authorization Code** as the security hand-shake between the source and target servers.



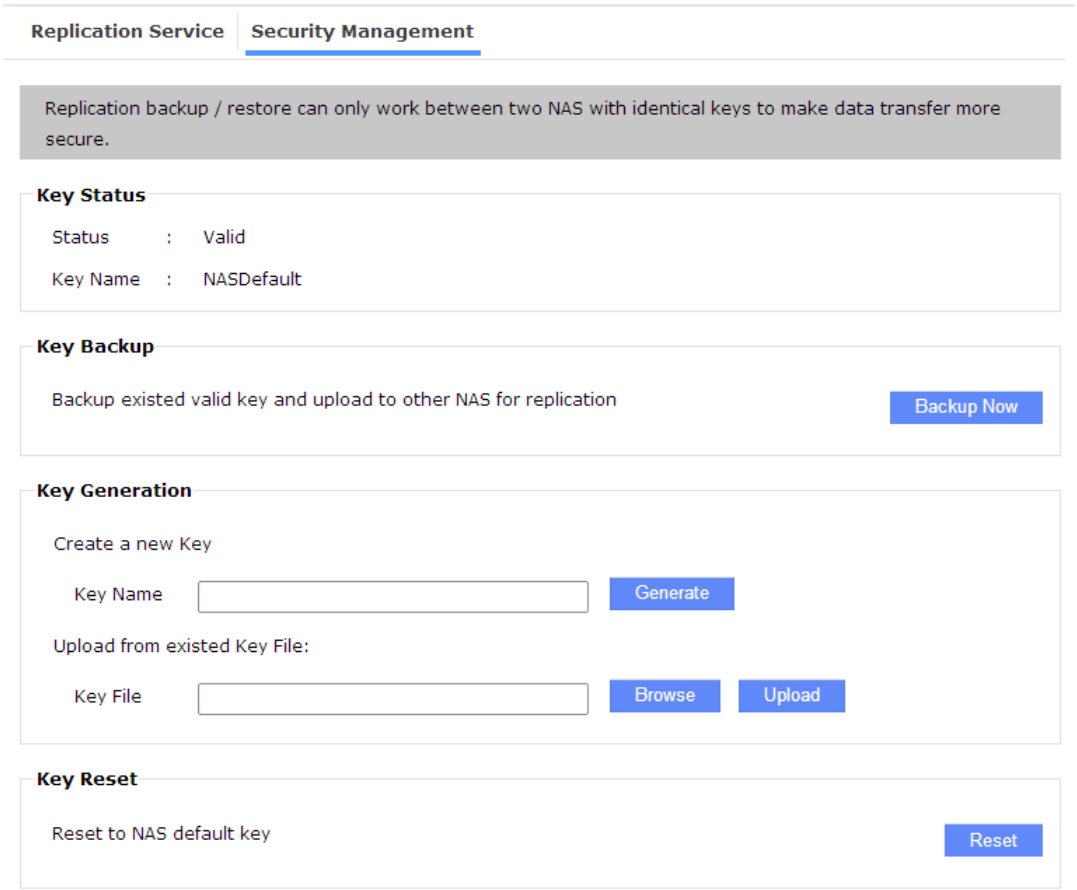
Make sure you create identical Service port and Authorization code on both the source and target serves.

Please refer to page 136 for details about **Backup** > **Replication** configuration.

The Replication service, after the initial full backup, replicates the data changes that take place after the initial replication to the target volume. In this way, only the data changes are moved to the target volume. Users can configure a replication schedule down to an interval as short as 10 minutes.



The **Security Management** window allows you to set up encrypted replication code and security key to ensure high security level when replicating data between two systems. Create encrypted key files and settings to share and secure the communications between two counterpart systems.



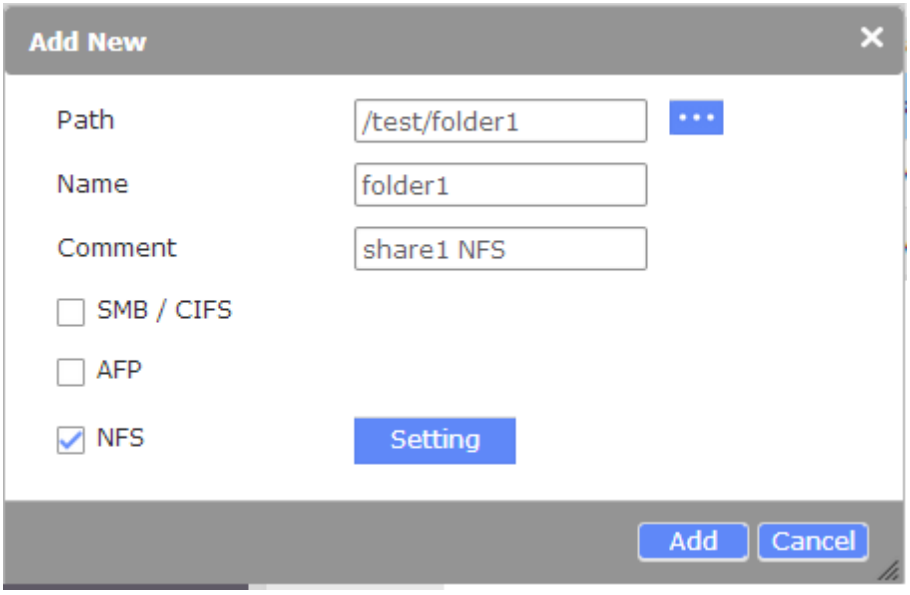
Chapter 7 Share

The Share window displays the currently available Folder Groups that are ready to provide shared storage over the network.

7.1. Share - Adding Shares

Once you create a Folder Group within a volume, you can create a share in the Share window by clicking the **Add** button.

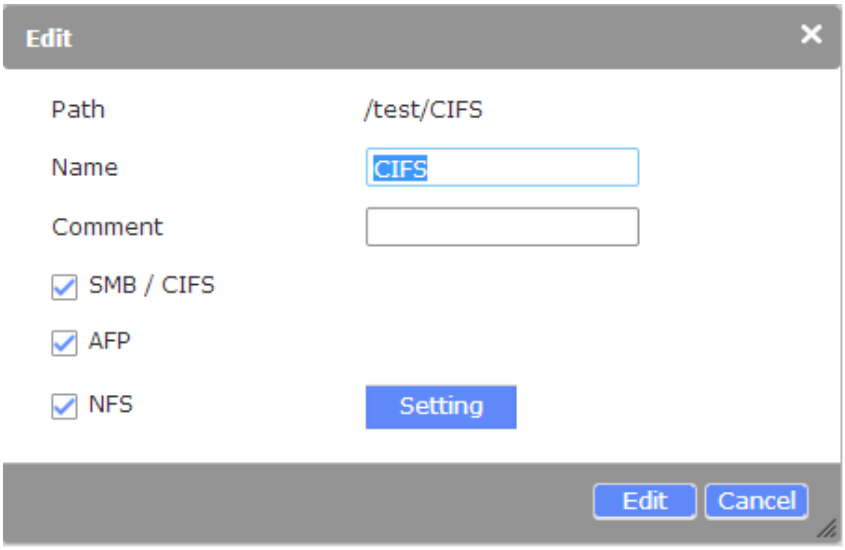
An Add New window will appear:
1. Click on the Find button on the right to select a directory under the storage volume (those that you created previously.) Select a Folder Group.
2. The **Name** of the Folder Group will appear automatically.
3. Add comments to the share, such as share1 for NFS.
4. Select a file system to which you want this share to be accessed.
5. Click the **Add** button to complete the process.



To examine the account who can access the share, you can click on the Permission button on the right to visit the Account > Permission window.

7.2. Share - Edit or Delete

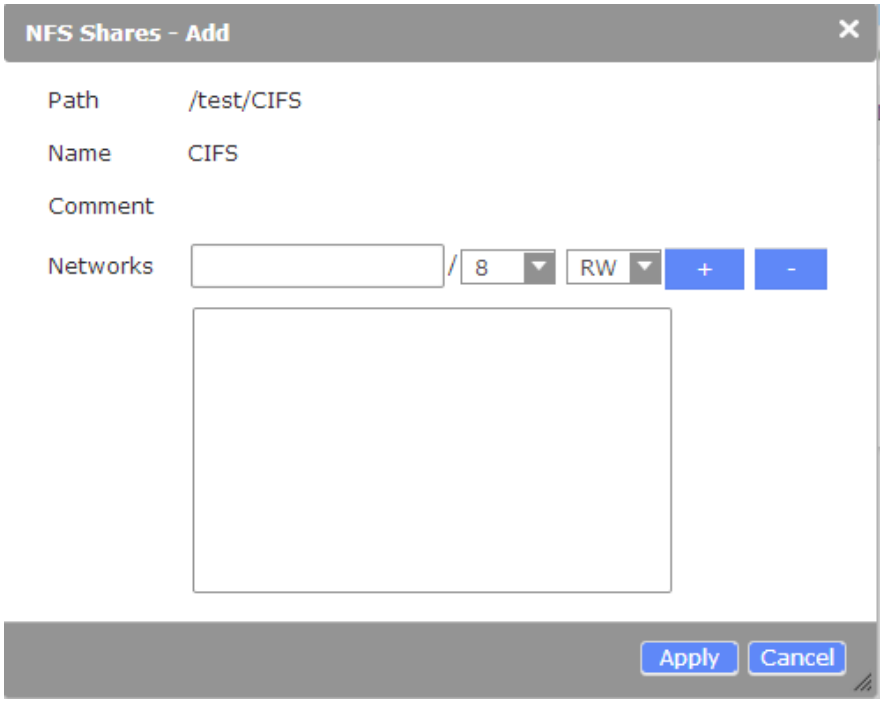
For a configured share, you can click on its checkbox to highlight your selection, and then click on the Edit button.



From here you can edit the share name, the comments, and the file system of the computers which can access this share.

For enabling a share for NFS-based computers, you can click on the Settings button, and enter a range of network addresses by enter the IP address, and selecting a Classless Inter-Domain Routing (CIDR) range. You can use online tools such as http://www.subnet-calculator.com/cidr.php to easily calculate a range of IP addresses. The Mask bits 8 allows 16,777,214 addresses, while Mask bit 24 allows 254 addresses.

Specify the Read/Write rights to the share and then click the "+" or "-" button to edit the access right attributes. Click the **Apply** button when done.



To delete a share, select the checkbox in front of it, and click the **Delete** button. The target Folder Group remains intact, only that it is not shared across the network.

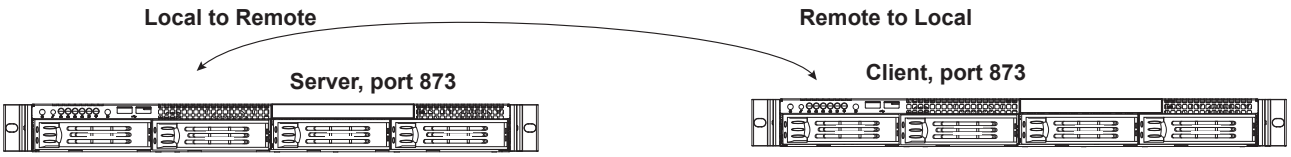
Chapter 8 Backup

The Backup window provides you with backup options such as Rsync, Local Copy, and Replication.

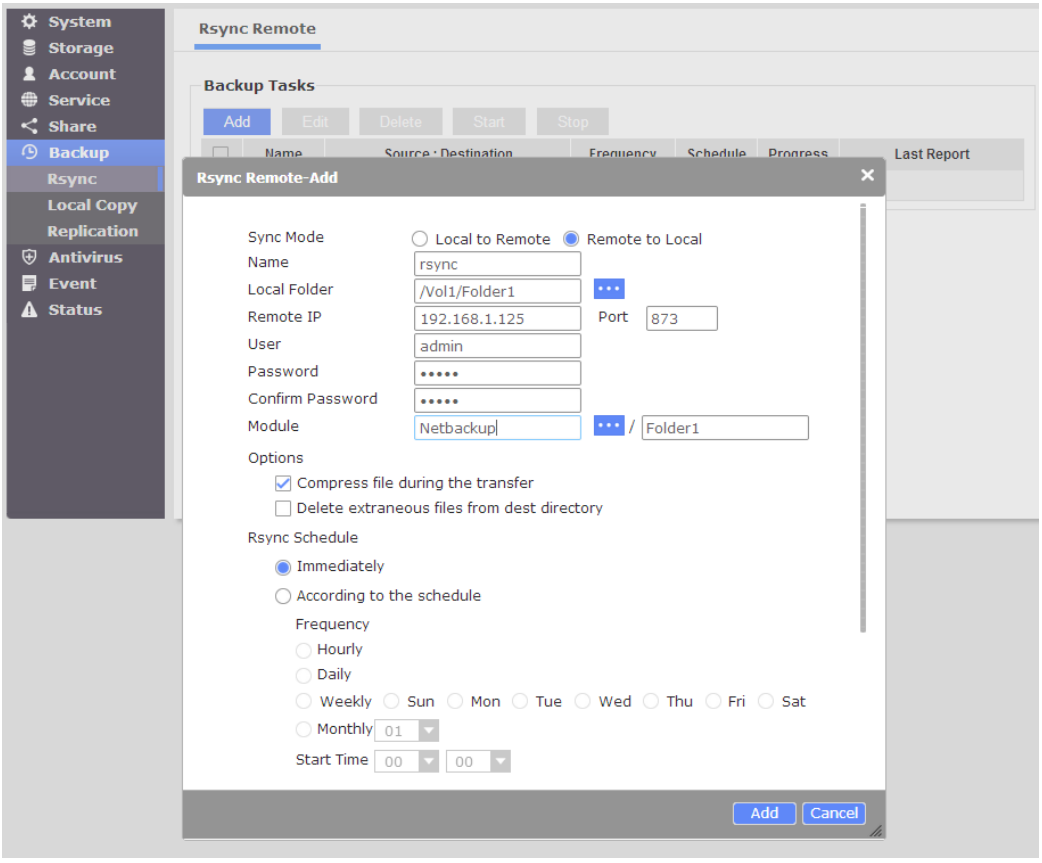
8.1. Backup - Rsync

Requirements:

1. You must have the **Rsync service** enabled as described on page **127**.
2. You must have a User account that is allowed the access to the directory to be backed up.
3. You must have another NAS server featuring twice the size of storage space than the Folder Group you want to back up. You should have access to both servers.



To run the Rsync operation, two or more NAS servers are required, one as the **Rsync server**, others as the **Rsync clients**.



1. Click on the **Add** button to display the Rsync configuration window.
2. Select the **Local to Remote** or the **Remote to Local** check circle.
3. Enter a **Name** for the Rsync configuration. Names must be identical on the server and on the client.
4. Select a **Local Folder Group** that you want to back up to a remote server.
5. Select a Remote IP where a synchronization Folder Group exists. Enter port number **873**.
6. Enter a User name that have a Full Access to the source Folder Group.
7. Enter and confirm the password for the user account.
8. Enter a Module name file. Default is **Netbackup**.
9. Select the **Compress file** option and/or the **Delete extraneous files** from destination directory.The extraneous files are those new ones on your server that haven't been backed up yet. The Delete extraneous files option is used when you want to restore an entire directory without the files changed after a specific point in time.
10. Rsync schedule:
    - 10-1. Immediately: Select this to start the Rsync immediately.
    - 10-2. According to the schedule:
      Select to Rsync hourly, Daily, Weekly, or according to the Monthly schedule. Each is done by selecting different check circles.

Once successfully started, you can check the Rsync progress in **Status** > **Task Progress** window. You can click on the details button to check the latest progress information.

NOTE:

The NAS server supports Rsync with the NAS server of the other brand which also supports rsync protocol. The other-brand NAS server may use other Rsync module for remote Rsync. When successfully connected to the other-band NAS server, the Rsync module of them will be displayed.

8.2. Backup - Local Copy

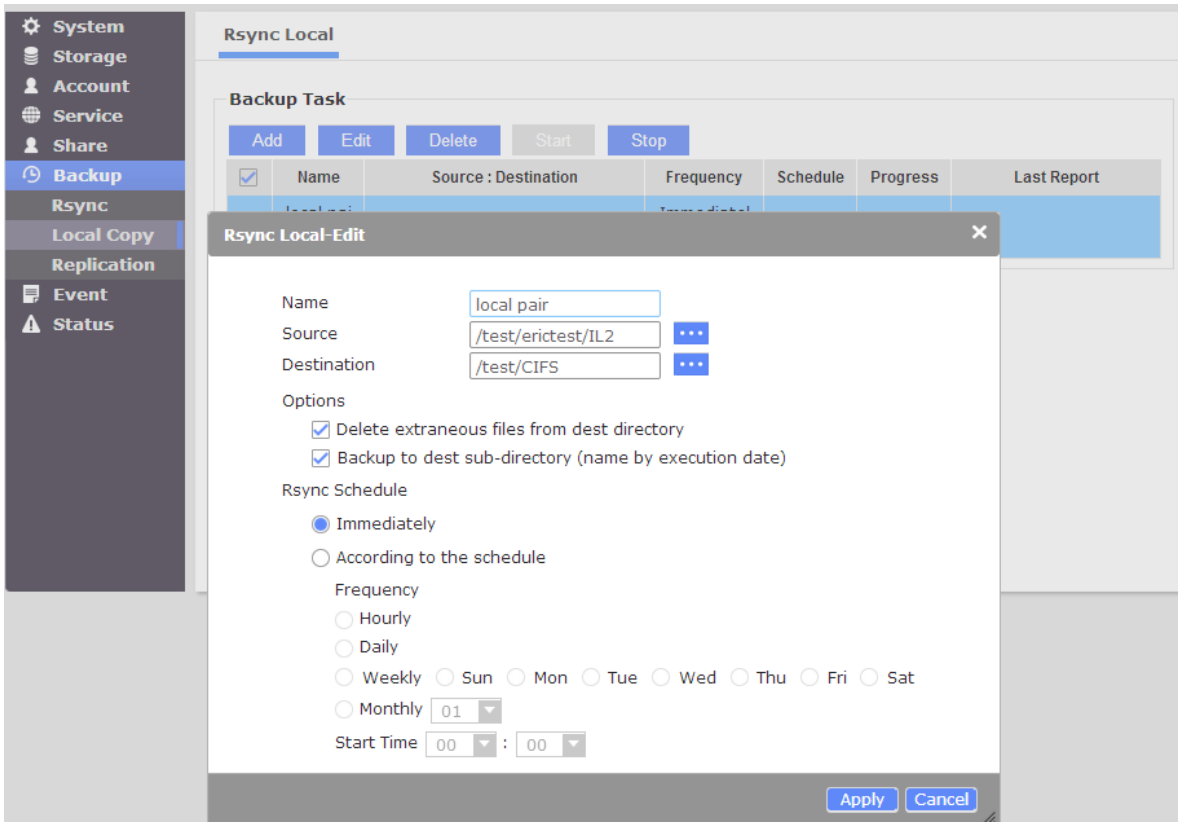
NOTE:
In addition to the copy from one Folder Group to anther, the Local Copy can be used to back up data to USB or eSATA devices. However, when backup is completed, please visit **Storage** > **Volume** > **External FAT/NTFS** to unmount the removable devices. This is in case that data inconsistency may occur.

Requirements:

1. You must have a Destination Folder Group that has a storage space equal or larger than the Source Folder Group. See page 127.

To add a backup task:
1. Click on the **Add** button. A Local Copy window will prompt.
2. Enter a name for the Local Copy task.
3. Select a Source Folder Group using the browse button.
4. Select a Destination Folder Group using the browse button.
5. Select the **Delete extraneous files** and/or the **Backup to dest. sub-directory** options. The extraneous files are those new ones on your server that haven't been backed up yet. The Delete extraneous files option is used when you want to restore an entire directory without the files changed after a specific point in time.

   When the backup to destination sub-directory option is selected, sub-directories will automatically be created according to the date/time each backup will take place.



6. Rsync schedule:
    6-1. Immediately: Select this to start the Rsync immediately.
    6-2. According to the schedule:
        Select to Rsync hourly, Daily, Weekly, or according to the Monthly schedule. Each is done by selecting different check circles.

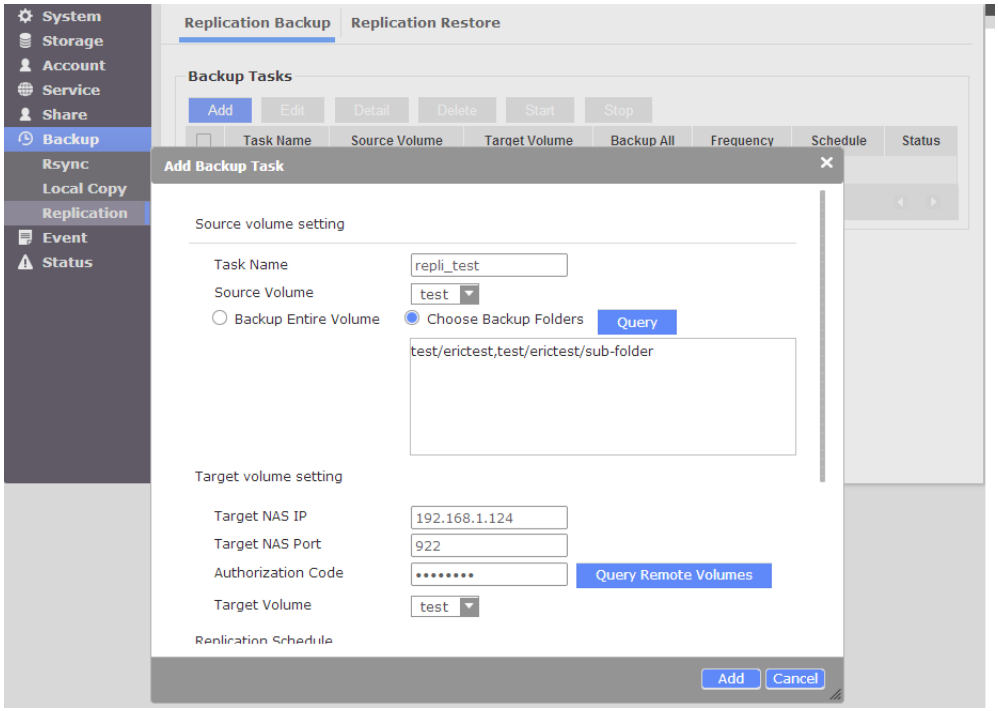
8.3. Backup - Replication

Requirements:

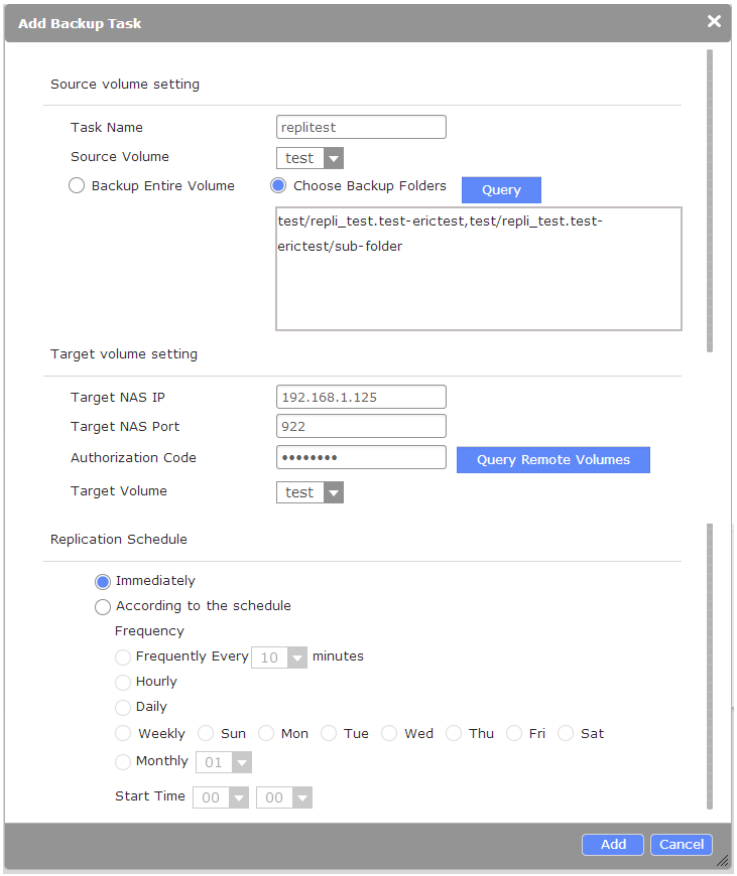
1. You must have the **Replication service** enabled as described on page **127**.
2. You must have another NAS server featuring a storage space equal or larger than the Folder Group you want to back up. You should have access to both servers.

The configuration procedure:

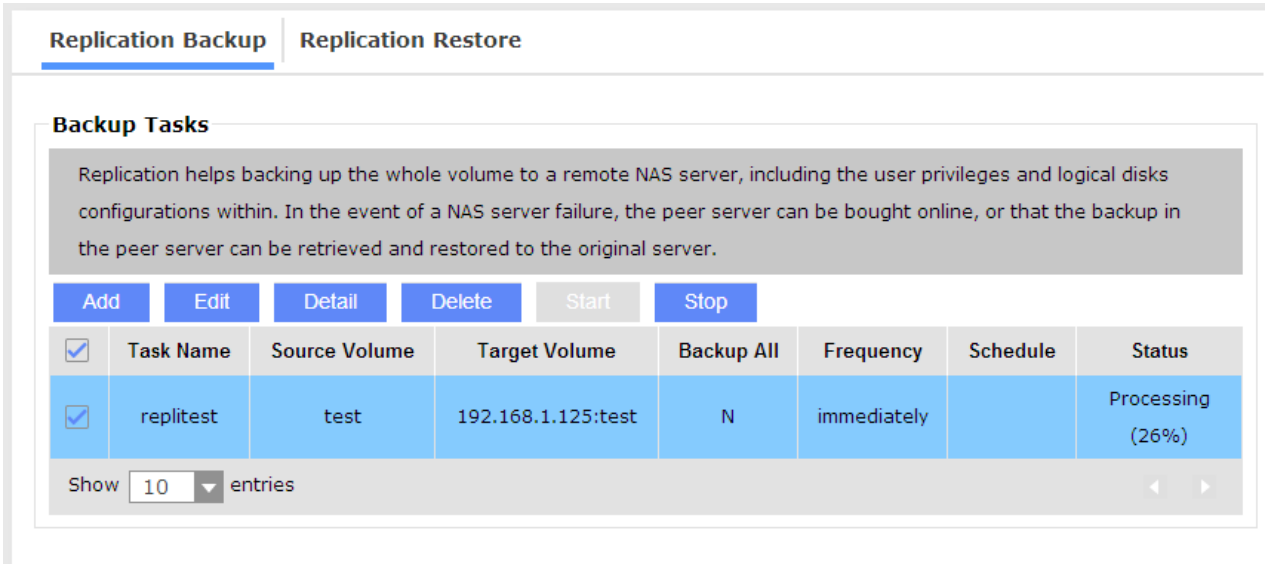
1. Enter a name for the **Task Name**.
2. Select a Source Volume (selected from the source NAS server). If you choose to back up a specific Folder Group, use the **Query** button to locate a Folder Group under a volume. When done, the Folder Group will be listed in the column below.
3. Enter the **Target NAS IP** (target NAS server), **Target NAS Port** (**922**), and the **Authorization Code** (one that is identical to the code you configured on the target NAS server).
4. You can use the **Query Remote Volumes** button to test the reachability of the target server.



5. The name of the **Target Volume** should automatically be polled if you enter the correct port number and the authorization code.
6. Replication schedule:
    6-1. **Immediately**: Select this to start the Rsync immediately.
    6-2. **According to the schedule**:
        Select to replicate data changes from source to target by minutes, or hourly, Daily, Weekly, or according to the Monthly schedule.
        Each is done by selecting different check circles.



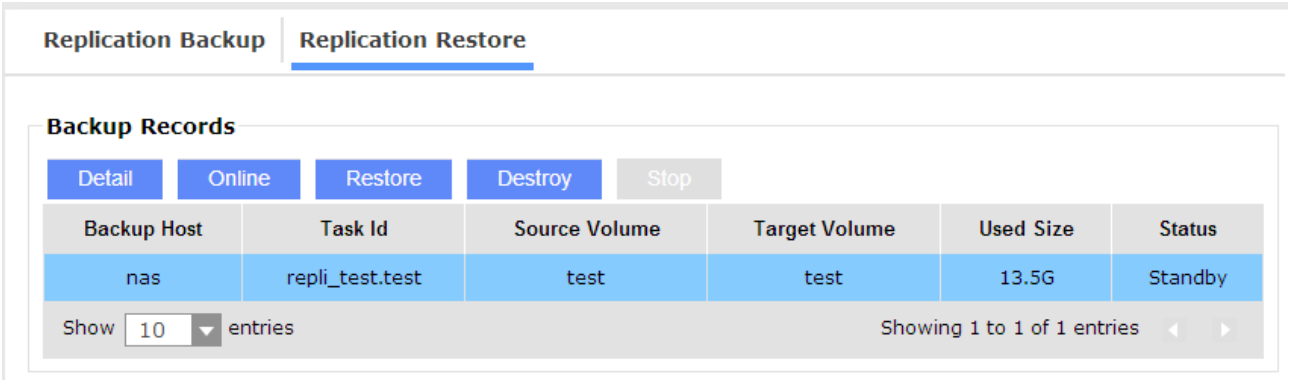
7. When done, you click on the **Add** button below to complete the configuration of a backup task.
8. You can then wait for several seconds, and click on the configured backup task to see processing status. You can then click on the **Start**, **Edit**, **Delete**, or **Stop** button to change its parameters. Normally, if a backup task is configured to be started immediately, after a short delay you should be able to see its progress on the **Status** column.



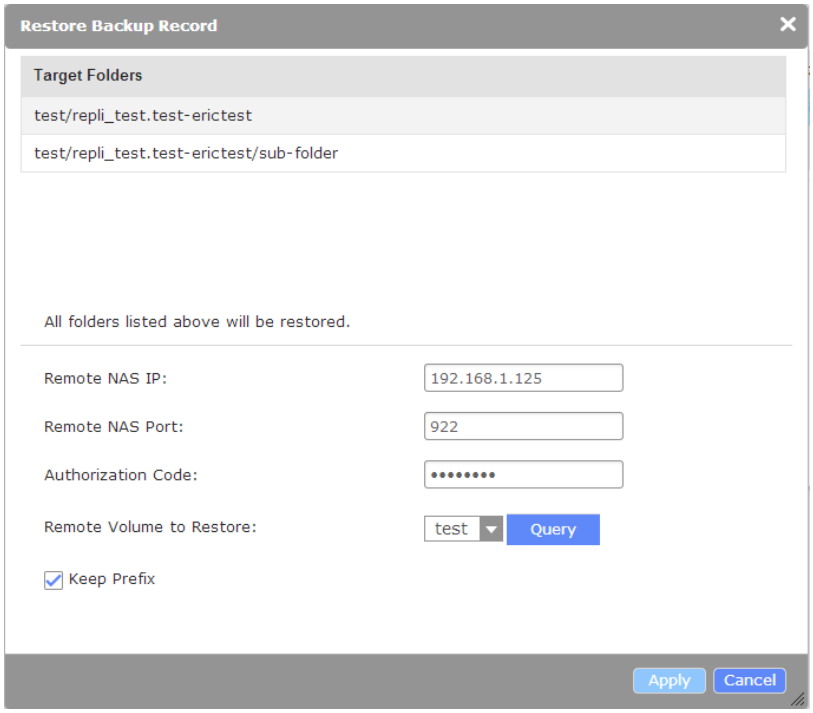
Backup - Replication Restore

The Replication Restore is performed on the target side. Once a replication backup is completed, and when you need to restore a backed-up replication on another server, click on the **Replication Restore** tabbed menu.

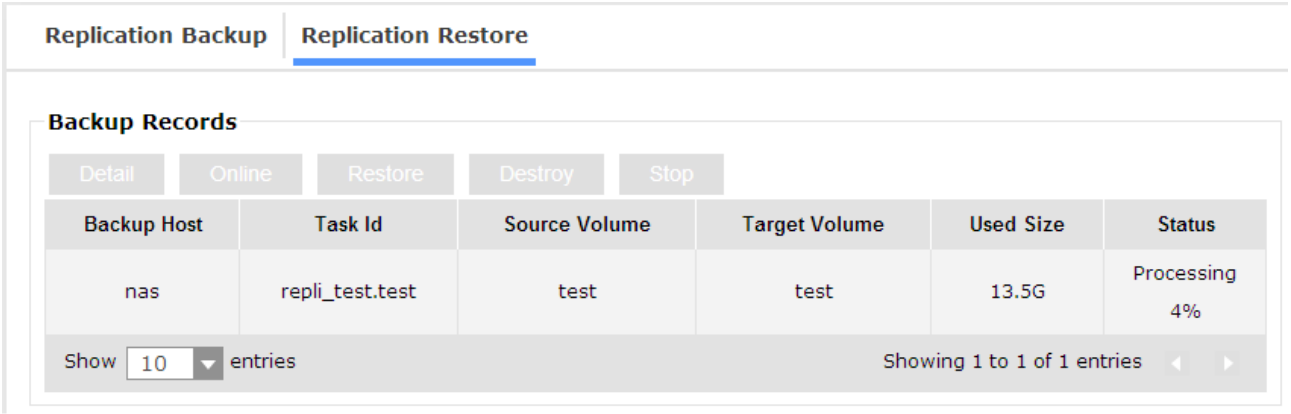
1. Click to select an existing replication configuration.
2. The **Detail**, **Online**, **Restore**, **Destroy**, and **Stop** tabs will appear.
3. Select a task to be performed from the tabbed menu.



4. If you select a Restore task, for example, the **Restore** menu will appear.
5. Enter the **Remote NAS IP**, NAS replication task **port**, **Authorization Code**, and you must ensure to click on the **Query** button to reach and list the reachable remote volume.
6. Click on the **Apply** button to begin the restoration task.



7. Click on the entry on the **Backup Records** menu to check its restoration progress.
8. When done, access the restored Folder Group to verify the correctness of the restored data.



Backup - Replication Online

Once a replication backup is completed, you can then bring the replicatin online on the target side. The Folder Group will be available for access.

NOTE:

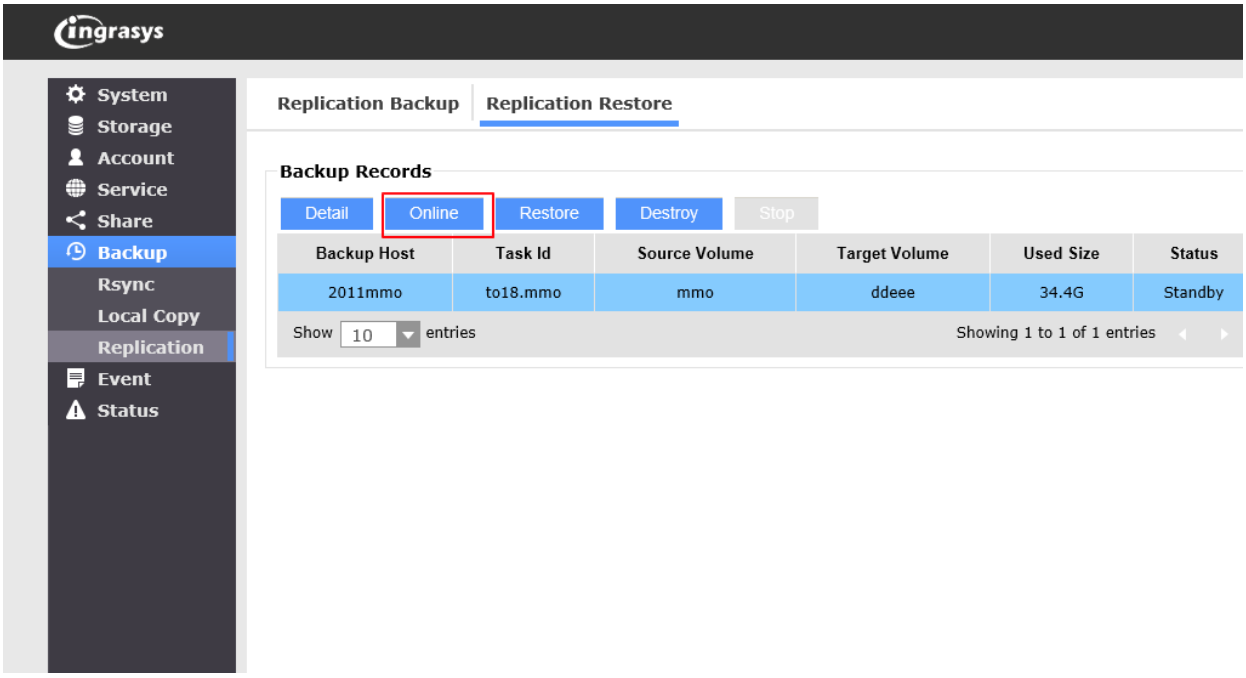
A. **Online** operation: Before being brought online, users can only export the replication as a Read-only share, and the existing replication schedule can incrementally back up the succeeding data changes according to a preset schedule. Once the users choose to turn the replication backup into the online state, the backup will become readable and writable, and hence the replication role will be depleted.

B. When you change a previously-completed replication into the Onlien state, and the replication starts to receive backup data, (e.g., when the scheduled backup time is reached), the replication backup will retrieve all data from the source. The replication process will start all over again. A new task entry will be listed at the Replciation Restore tab window.

C. If you should destroy a replication backup, the destroy action will erase not only the replication record but also all data created and associated with the replication task.

The online procedure:

1. Click the **Online** button.
2. You will then be able to use the Folder Group as an online share.



Chapter 9 Antivirus

The built-in ClamAV antivirus software provides protection to virus attack against various types of virus.

9.1. Antivirus > Information

This page provides the information showing the current virus code, virus scan work record, and antivirus configuration details.

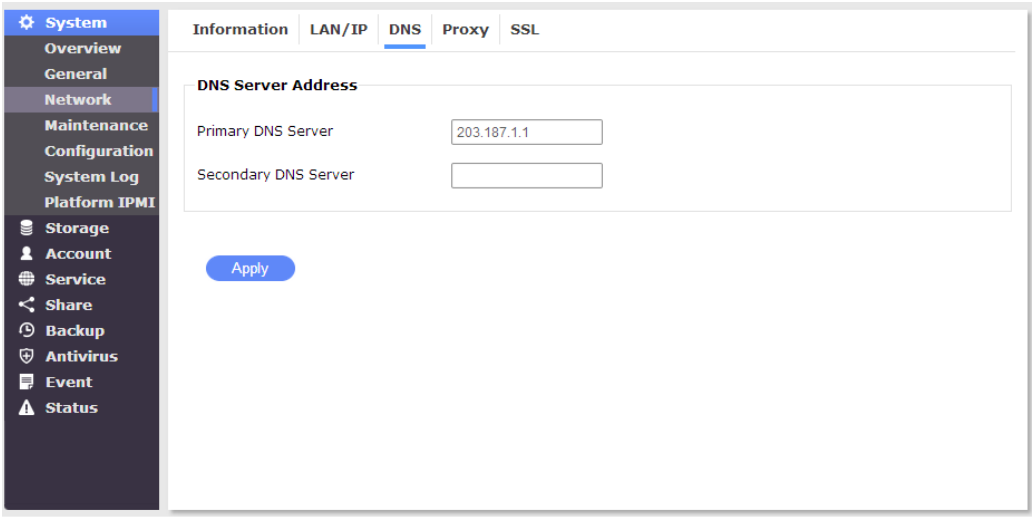
9.2. Antivirus > Antivirus Tasks

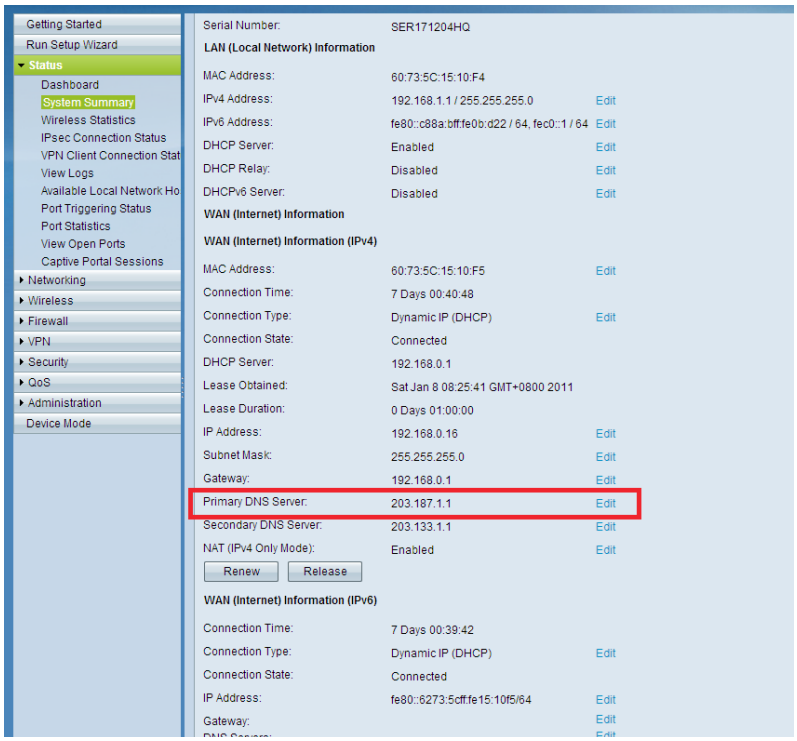
This page provides access to manual or scheduled virus scan.

Please note the following before proceeding with the anitvirus configuration:

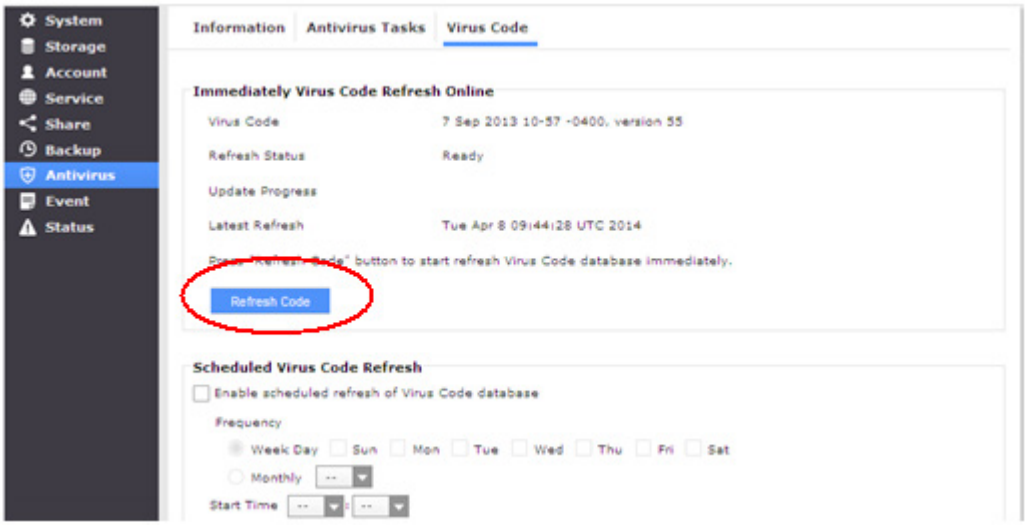
NOTE:

1. **Your system first first must have a System Volume before you can apply the antivirus function. See Storag > Volume on page 78 for details.**
2. Before you can make use the anivirus function, please visit the **Antivirus > Virus Code** to gain access to the latest virous code. Otherwise, the antivirus code will not take effect.
3. Make sure you have configured the correct DNS server address in **System > Network > DNS Server Address**.



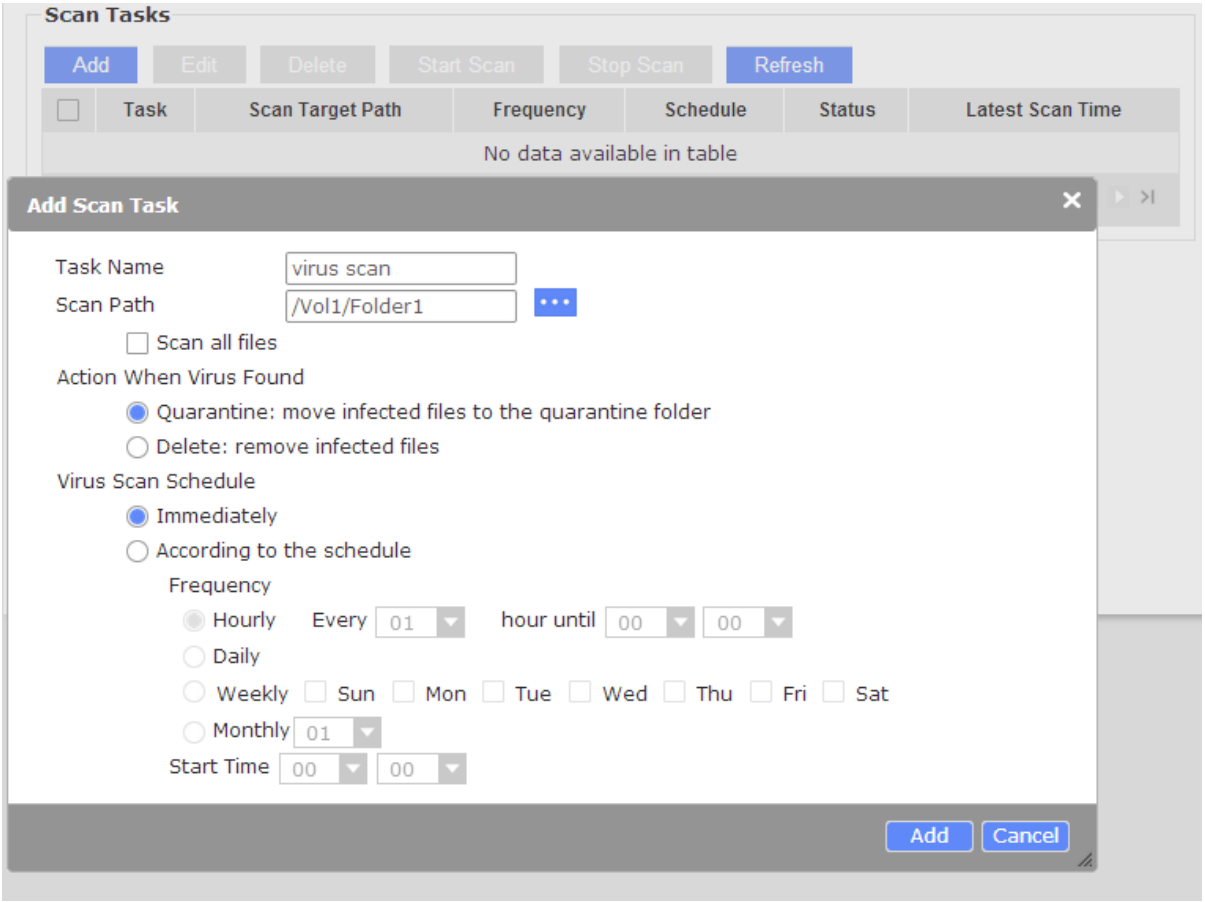


Click on the **Refresh Code** button to enable the antivirus function.



To begin a manual or scheduled scan,

1. Click the **Add** button.
2. Enter the name for the task.
3. Select from the **Scan Path** menu and/or the Scan all files option for which part of your volume needs to be scanned (and the sub-directories).
4. Select the **Immediately** checkbox to begin the scan task immediately, or configure the intervals for the virus scan schedule using the configuration options below.



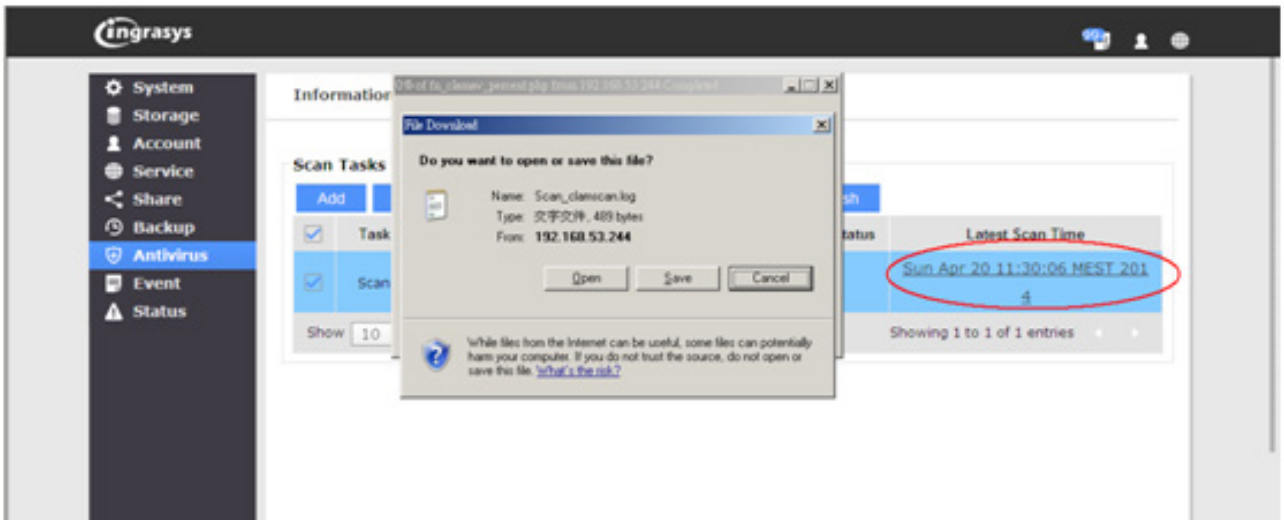
To configure the anti-virus-related settings
1. Action when virus found - Quarantine - move infected files to the quarantine folder.
- Delete: remove affected files.
Please note that even compressed files or folders can be scanned, and the virus can be found.

2. Click the Add button for the configuration to take effect.

9.3. Antivirus > Virus Scan Record

All virus scan record shall include the following:

1. Number of scanned files and directories.
2. Number of affected files.
3. A list of affected files.
4. The time record of when the antivirus scan took place.
5. To view the record file, enter the **Antivirus** > **Antivirus Task** > **Latest Scan Time**.
6. Click on the shortcut to open or save the record file.



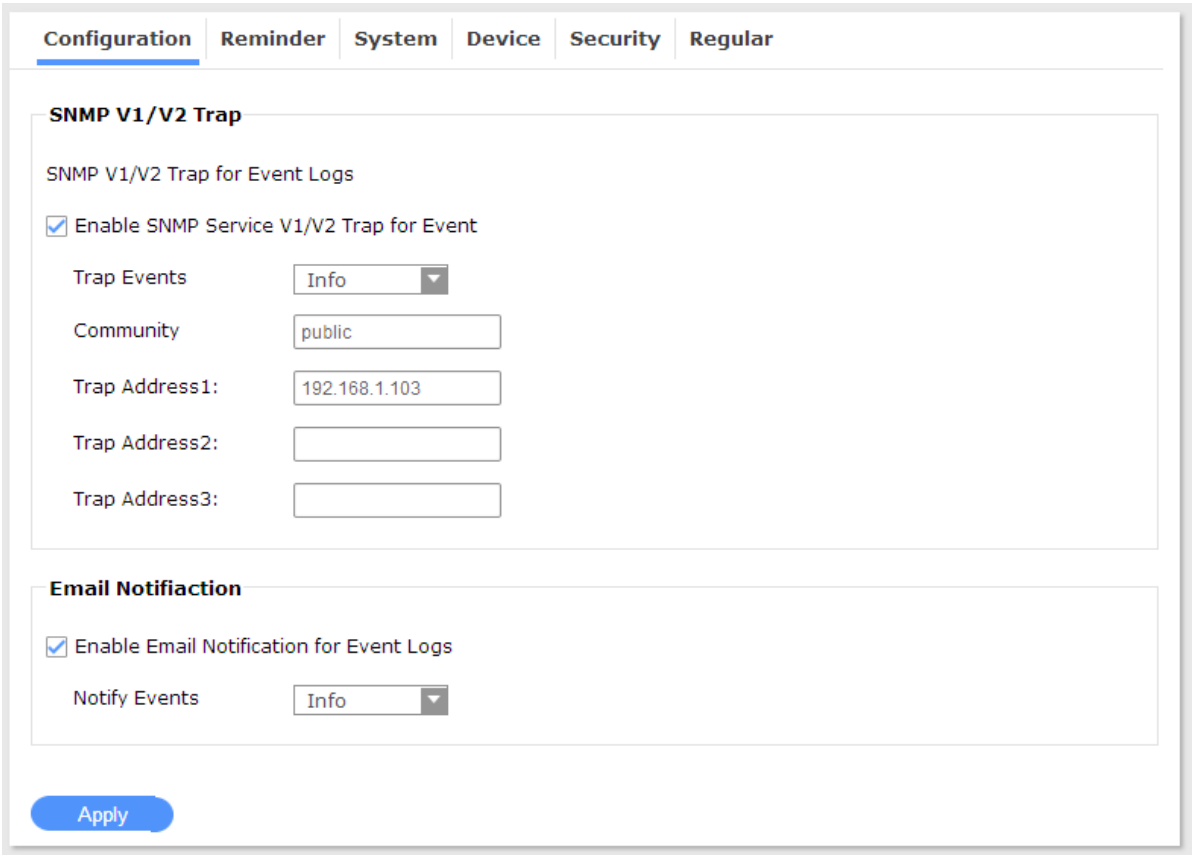
Chapter 10 Event

The Event windows provides access to all system events concerning configuration changes, reminder, System-related, Device-related, Security, and Regular messages.

10.1. Event > Configuration

Once you enter the Event window, the system will default to the **Reminder** screen, instead of the Configuration screen.

To enter Configuration page, click on the **Configuration** tab.



The **SNMP V1/V2 Trap** column determines which level of event messages, in which community, and which IP address will be receiving the SNMP trap messages.

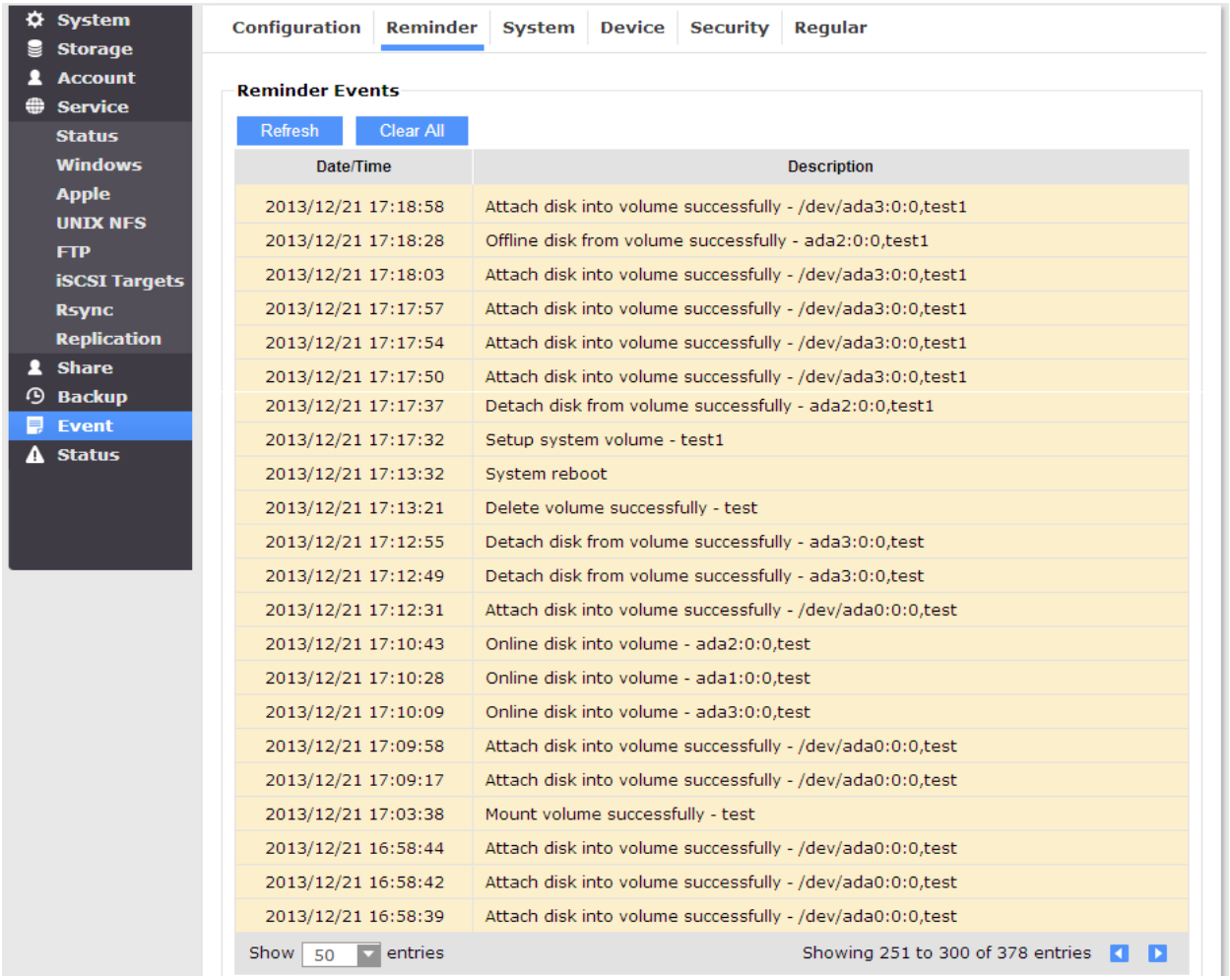
Note that the **Trap Events** setup determines what level of event messages the trap receivers will receive. For example, if you designate **Info**, events of all event levels starting from **Info**, **Warning**, to **Error** will be delivered to the receivers. If only the **Error** level is configured here, only the most critical events, that of the Error level, will be delivered to the receivers.

Email Notification

The event messages can be delivered through Email. Select from the **Notify Events** drop-down box which severity level of events will be delivered to the receiver. The severity level can be **Info**, **Warning**, or **Error**.

10.2. Event > Reminder

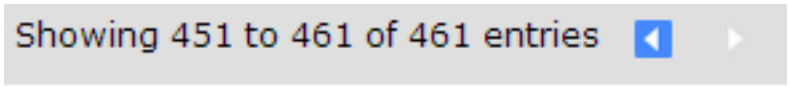
The Reminder events include system critical events such as component failures or major events, e.g., firmware update, mount/unmount volume, system reboot, creation/deletion of folders or logical disks, add/remove disks, volume rebuild, etc.

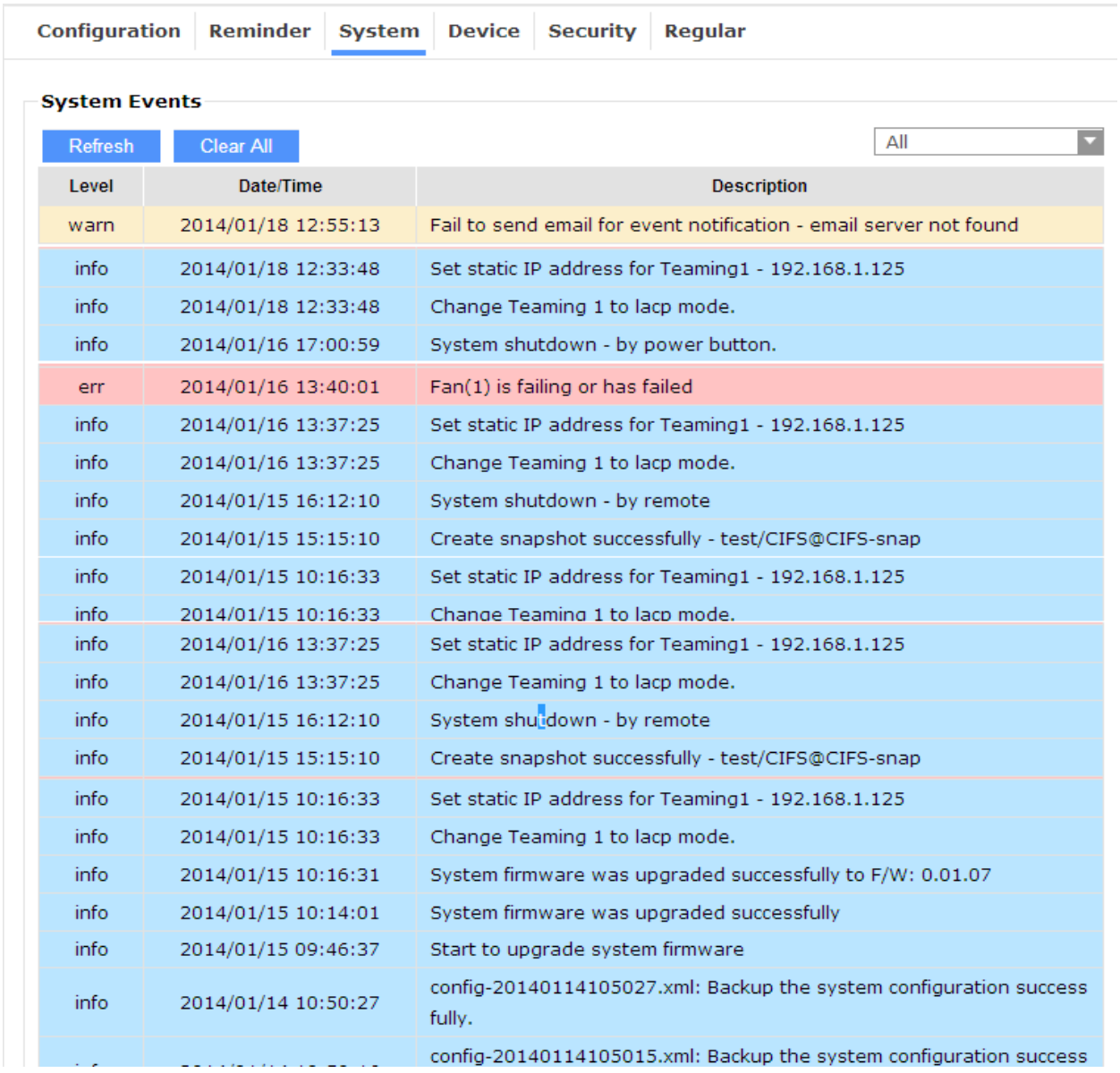

System
Storage
Account
Service
Status
Windows
Apple
UNIX NFS
FTP
iSCSI Targets
Rsync
Replication
Share
Backup
Event
Status
Configuration
Reminder
System
Device
Security
Regular
Reminder Events
Refresh
Clear All
Date/Time
Description
2013/12/21 17:18:58 Attach disk into volume successfully - /dev/ada3:0:0,test1
2013/12/21 17:18:28 Offline disk from volume successfully - ada2:0:0,test1
2013/12/21 17:18:03 Attach disk into volume successfully - /dev/ada3:0:0,test1
2013/12/21 17:17:57 Attach disk into volume successfully - /dev/ada3:0:0,test1
2013/12/21 17:17:54 Attach disk into volume successfully - /dev/ada3:0:0,test1
2013/12/21 17:17:50 Attach disk into volume successfully - /dev/ada3:0:0,test1
2013/12/21 17:17:37 Detach disk from volume successfully - ada2:0:0,test1
2013/12/21 17:17:32 Setup system volume - test1
2013/12/21 17:13:32 System reboot
2013/12/21 17:13:21 Delete volume successfully - test
2013/12/21 17:12:55 Detach disk from volume successfully - ada3:0:0,test
2013/12/21 17:12:49 Detach disk from volume successfully - ada3:0:0,test
2013/12/21 17:12:31 Attach disk into volume successfully - /dev/ada0:0:0,test
2013/12/21 17:10:43 Online disk into volume - ada2:0:0,test
2013/12/21 17:10:28 Online disk into volume - ada1:0:0,test
2013/12/21 17:10:09 Online disk into volume - ada3:0:0,test
2013/12/21 17:09:58 Attach disk into volume successfully - /dev/ada0:0:0,test
2013/12/21 17:09:17 Attach disk into volume successfully - /dev/ada0:0:0,test
2013/12/21 17:03:38 Mount volume successfully - test
2013/12/21 16:58:44 Attach disk into volume successfully - /dev/ada0:0:0,test
2013/12/21 16:58:42 Attach disk into volume successfully - /dev/ada0:0:0,test
2013/12/21 16:58:39 Attach disk into volume successfully - /dev/ada0:0:0,test
Show 50 entries
Showing 251 to 300 of 378 entries

10.3. Event > System

The System events include system-related events such as component failures, network-related configuration, system on/off, firmware update, reboot, volume configuration, etc.

Use the page up and page down button to move to other event pages.

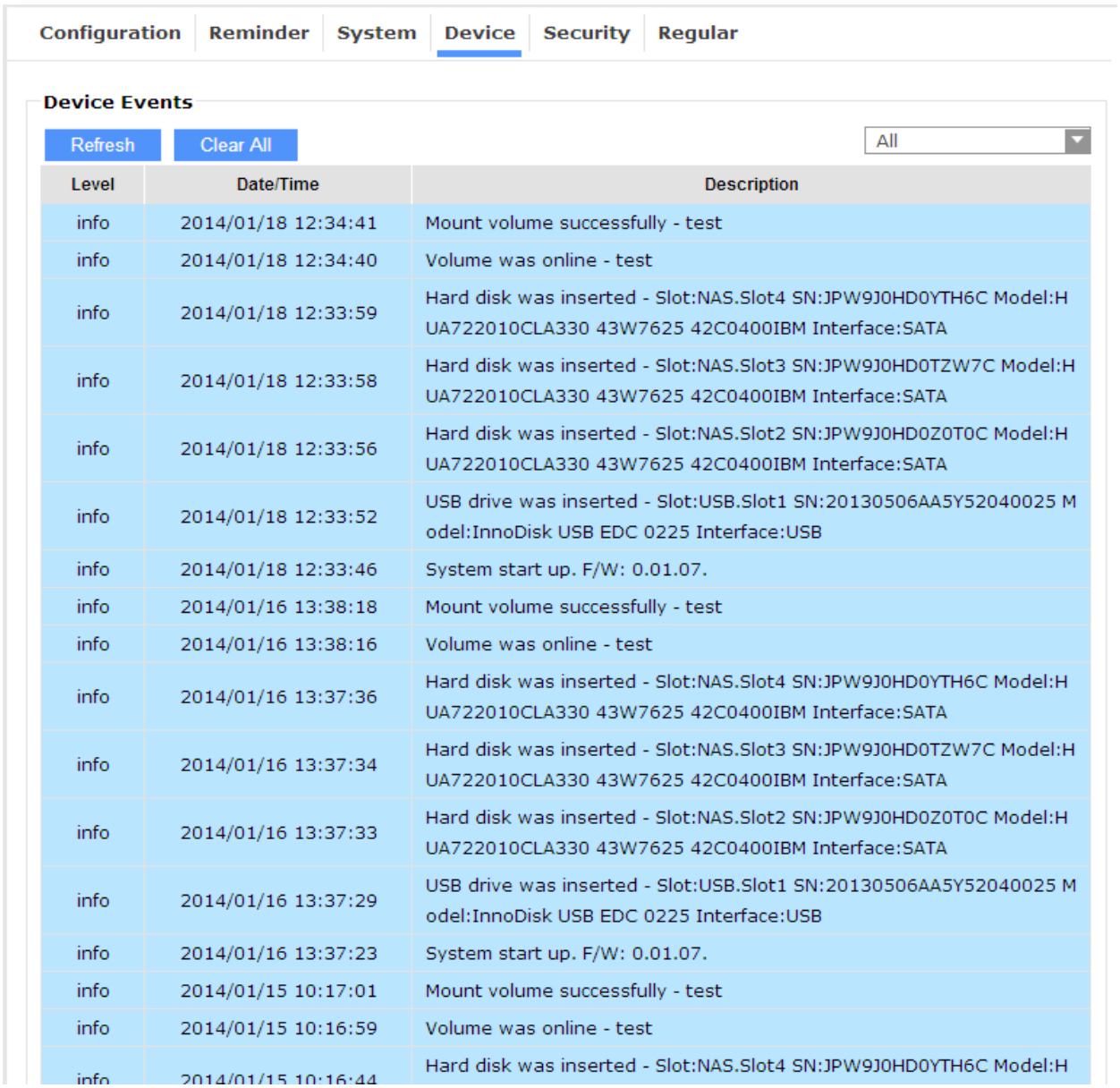




Level	Date/Time	Description
warn	2014/01/18 12:55:13	Fail to send email for event notification - email server not found
info	2014/01/18 12:33:48	Set static IP address for Teaming1 - 192.168.1.125
info	2014/01/18 12:33:48	Change Teaming 1 to lacp mode.
info	2014/01/16 17:00:59	System shutdown - by power button.
err	2014/01/16 13:40:01	Fan(1) is failing or has failed
info	2014/01/16 13:37:25	Set static IP address for Teaming1 - 192.168.1.125
info	2014/01/16 13:37:25	Change Teaming 1 to lacp mode.
info	2014/01/15 16:12:10	System shutdown - by remote
info	2014/01/15 15:15:10	Create snapshot successfully - test/CIFS@CIFS-snap
info	2014/01/15 10:16:33	Set static IP address for Teaming1 - 192.168.1.125
info	2014/01/15 10:16:33	Change Teaming 1 to lacp mode.
info	2014/01/16 13:37:25	Set static IP address for Teaming1 - 192.168.1.125
info	2014/01/16 13:37:25	Change Teaming 1 to lacp mode.
info	2014/01/15 16:12:10	System shutdown - by remote
info	2014/01/15 15:15:10	Create snapshot successfully - test/CIFS@CIFS-snap
info	2014/01/15 10:16:33	Set static IP address for Teaming1 - 192.168.1.125
info	2014/01/15 10:16:33	Change Teaming 1 to lacp mode.
info	2014/01/15 10:16:31	System firmware was upgraded successfully to F/W: 0.01.07
info	2014/01/15 10:14:01	System firmware was upgraded successfully
info	2014/01/15 09:46:37	Start to upgrade system firmware
info	2014/01/14 10:50:27	config-20140114105027.xml: Backup the system configuration success fully.
		config-20140114105015.xml: Backup the system configuration success

10.4. Event > Device

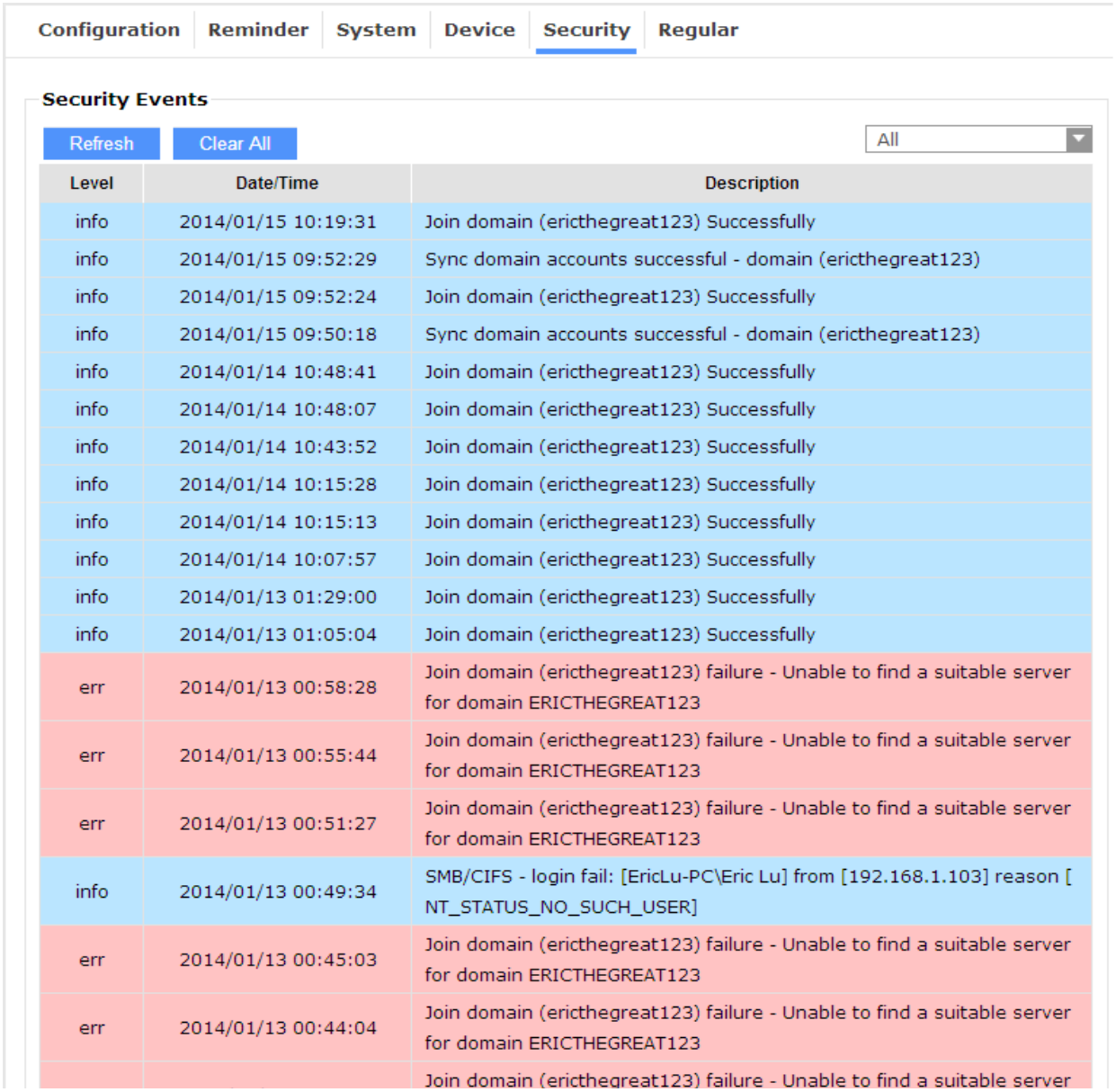
The Device events include those for system volumes, hard disks, system start time, USB drive operation, eSATA devices,



Level	Date/Time	Description
info	2014/01/18 12:34:41	Mount volume successfully - test
info	2014/01/18 12:34:40	Volume was online - test
info	2014/01/18 12:33:59	Hard disk was inserted - Slot:NAS.Slot4 SN:JPW9J0HD0YTH6C Model:HUA722010CLA330 43W7625 42C0400IBM Interface:SATA
info	2014/01/18 12:33:58	Hard disk was inserted - Slot:NAS.Slot3 SN:JPW9J0HD0TZW7C Model:HUA722010CLA330 43W7625 42C0400IBM Interface:SATA
info	2014/01/18 12:33:56	Hard disk was inserted - Slot:NAS.Slot2 SN:JPW9J0HD0Z0T0C Model:HUA722010CLA330 43W7625 42C0400IBM Interface:SATA
info	2014/01/18 12:33:52	USB drive was inserted - Slot:USB.Slot1 SN:20130506AA5Y52040025 Model:InnoDisk USB EDC 0225 Interface:USB
info	2014/01/18 12:33:46	System start up. F/W: 0.01.07.
info	2014/01/16 13:38:18	Mount volume successfully - test
info	2014/01/16 13:38:16	Volume was online - test
info	2014/01/16 13:37:36	Hard disk was inserted - Slot:NAS.Slot4 SN:JPW9J0HD0YTH6C Model:HUA722010CLA330 43W7625 42C0400IBM Interface:SATA
info	2014/01/16 13:37:34	Hard disk was inserted - Slot:NAS.Slot3 SN:JPW9J0HD0TZW7C Model:HUA722010CLA330 43W7625 42C0400IBM Interface:SATA
info	2014/01/16 13:37:33	Hard disk was inserted - Slot:NAS.Slot2 SN:JPW9J0HD0Z0T0C Model:HUA722010CLA330 43W7625 42C0400IBM Interface:SATA
info	2014/01/16 13:37:29	USB drive was inserted - Slot:USB.Slot1 SN:20130506AA5Y52040025 Model:InnoDisk USB EDC 0225 Interface:USB
info	2014/01/16 13:37:23	System start up. F/W: 0.01.07.
info	2014/01/15 10:17:01	Mount volume successfully - test
info	2014/01/15 10:16:59	Volume was online - test
info	2014/01/15 10:16:44	Hard disk was inserted - Slot:NAS.Slot4 SN:JPW9J0HD0YTH6C Model:H

10.5. Event > Security

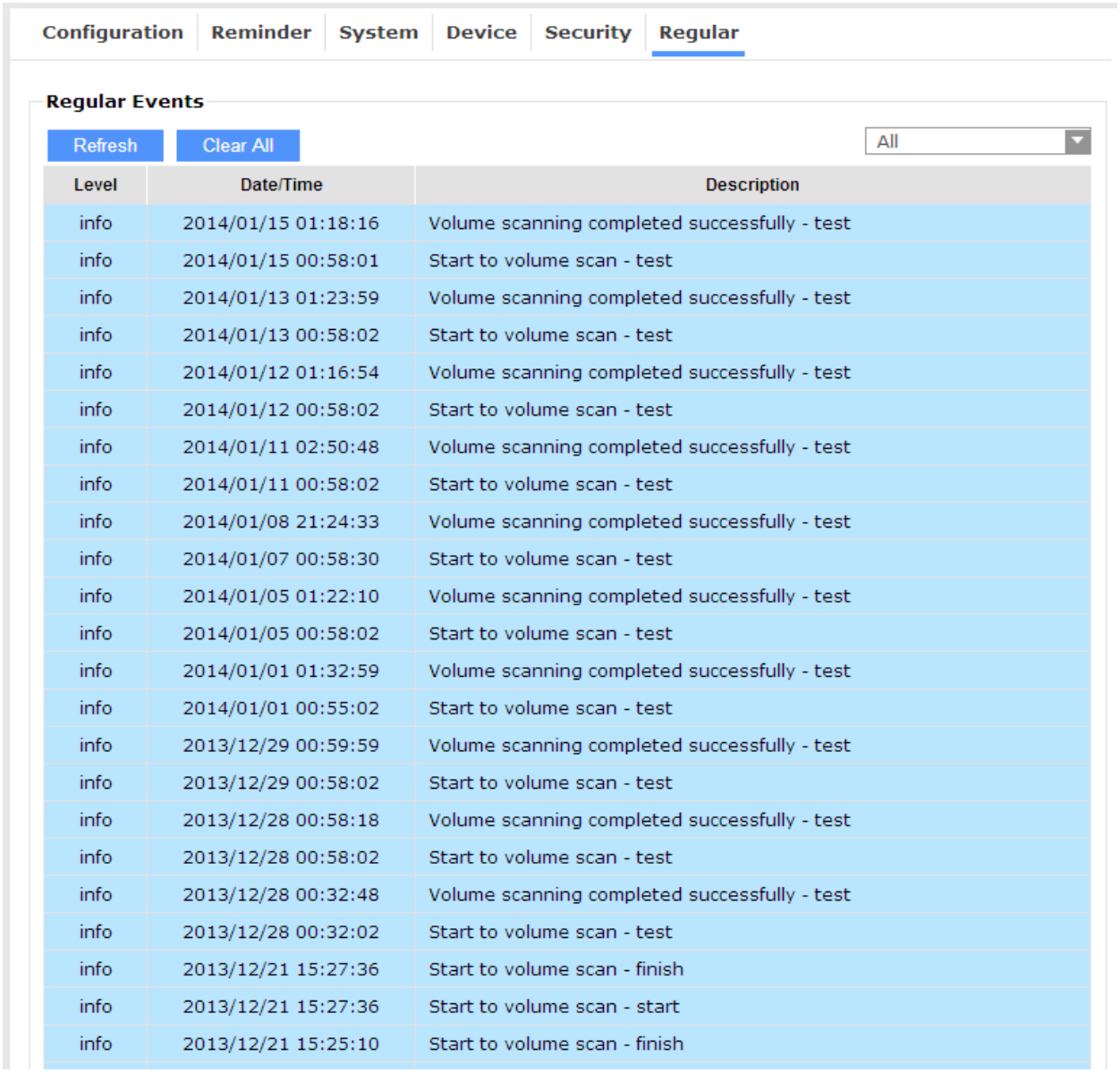
The Security events include those for access rights, including domain configuration, login status, domain information synchronization, user's permission succeed/failure, etc.



Level	Date/Time	Description
info	2014/01/15 10:19:31	Join domain (ericthegreat123) Successfully
info	2014/01/15 09:52:29	Sync domain accounts successful - domain (ericthegreat123)
info	2014/01/15 09:52:24	Join domain (ericthegreat123) Successfully
info	2014/01/15 09:50:18	Sync domain accounts successful - domain (ericthegreat123)
info	2014/01/14 10:48:41	Join domain (ericthegreat123) Successfully
info	2014/01/14 10:48:07	Join domain (ericthegreat123) Successfully
info	2014/01/14 10:43:52	Join domain (ericthegreat123) Successfully
info	2014/01/14 10:15:28	Join domain (ericthegreat123) Successfully
info	2014/01/14 10:15:13	Join domain (ericthegreat123) Successfully
info	2014/01/14 10:07:57	Join domain (ericthegreat123) Successfully
info	2014/01/13 01:29:00	Join domain (ericthegreat123) Successfully
info	2014/01/13 01:05:04	Join domain (ericthegreat123) Successfully
err	2014/01/13 00:58:28	Join domain (ericthegreat123) failure - Unable to find a suitable server for domain ERICTHEGREAT123
err	2014/01/13 00:55:44	Join domain (ericthegreat123) failure - Unable to find a suitable server for domain ERICTHEGREAT123
err	2014/01/13 00:51:27	Join domain (ericthegreat123) failure - Unable to find a suitable server for domain ERICTHEGREAT123
info	2014/01/13 00:49:34	SMB/CIFS - login fail: [EricLu-PC\Eric Lu] from [192.168.1.103] reason [NT_STATUS_NO_SUCH_USER]
err	2014/01/13 00:45:03	Join domain (ericthegreat123) failure - Unable to find a suitable server for domain ERICTHEGREAT123
err	2014/01/13 00:44:04	Join domain (ericthegreat123) failure - Unable to find a suitable server for domain ERICTHEGREAT123
		Join domain (ericthegreat123) failure - Unable to find a suitable server

10.6. Event > Regular

The Regular events mostly include those for system maintenance schedule such as scheduled tasks such as snapshot and Rsync.



Level	Date/Time	Description
info	2014/01/15 01:18:16	Volume scanning completed successfully - test
info	2014/01/15 00:58:01	Start to volume scan - test
info	2014/01/13 01:23:59	Volume scanning completed successfully - test
info	2014/01/13 00:58:02	Start to volume scan - test
info	2014/01/12 01:16:54	Volume scanning completed successfully - test
info	2014/01/12 00:58:02	Start to volume scan - test
info	2014/01/11 02:50:48	Volume scanning completed successfully - test
info	2014/01/11 00:58:02	Start to volume scan - test
info	2014/01/08 21:24:33	Volume scanning completed successfully - test
info	2014/01/07 00:58:30	Start to volume scan - test
info	2014/01/05 01:22:10	Volume scanning completed successfully - test
info	2014/01/05 00:58:02	Start to volume scan - test
info	2014/01/01 01:32:59	Volume scanning completed successfully - test
info	2014/01/01 00:55:02	Start to volume scan - test
info	2013/12/29 00:59:59	Volume scanning completed successfully - test
info	2013/12/29 00:58:02	Start to volume scan - test
info	2013/12/28 00:58:18	Volume scanning completed successfully - test
info	2013/12/28 00:58:02	Start to volume scan - test
info	2013/12/28 00:32:48	Volume scanning completed successfully - test
info	2013/12/28 00:32:02	Start to volume scan - test
info	2013/12/21 15:27:36	Start to volume scan - finish
info	2013/12/21 15:27:36	Start to volume scan - start
info	2013/12/21 15:25:10	Start to volume scan - finish

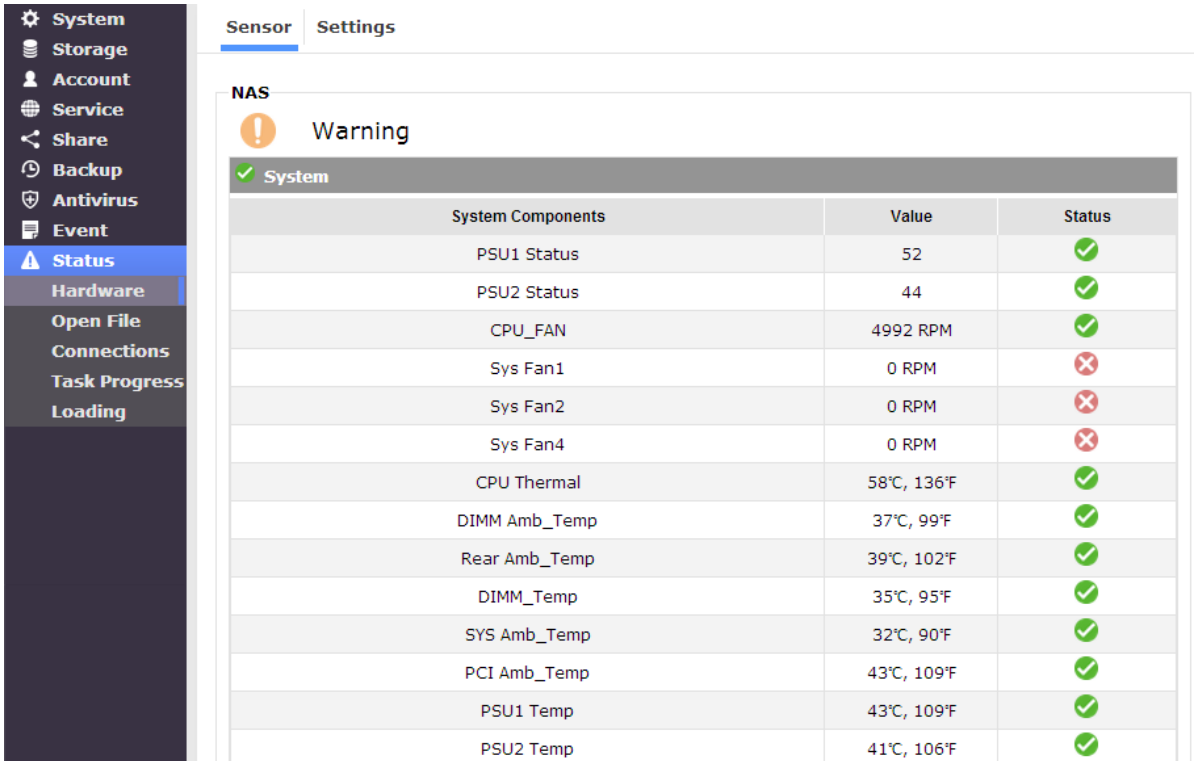
Chapter 11 Status

The Status windows provides a glimpse of hardware, access to network shares, connections, scheduled task progress, and system loading.

11.1. Hardware

All important system operating statuses are listed here. Their statuses indicated by green or red indicators. CPU thermal, power input, and fan rotation speed are automatically detected and reported in here.

This window also comes with a Location LED button, when pressed, the ID LED on system front panel will light up, showing the maintenance personnel of the location of the system. The LED will constantly light blue until the ID button is pressed for 1 second.



Settings

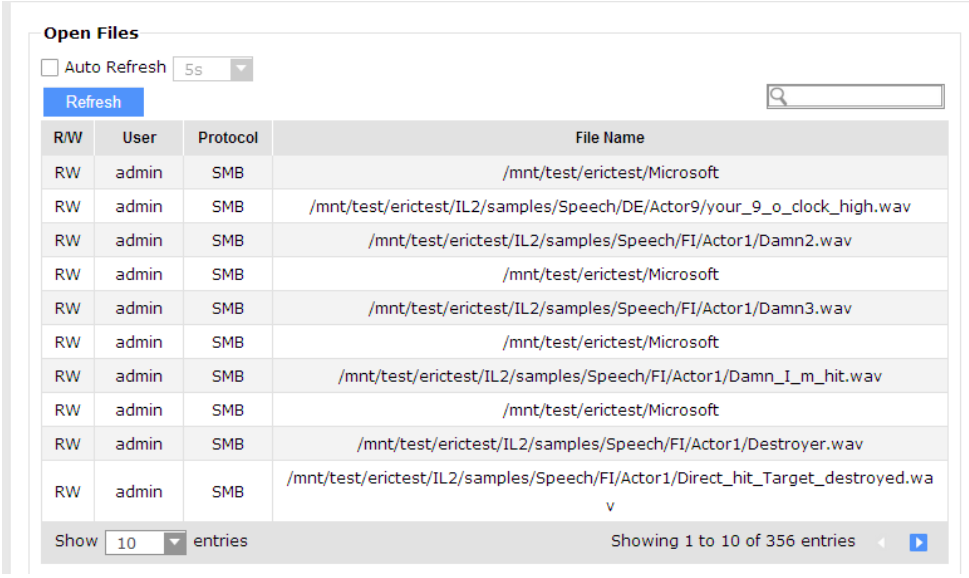
Enable notification: Click to enable system status notification via Emails and other notification method.

Enable critical shutdown: Click to enable automated shutdown when system encounters critical system faults, such as unsteady power inputs or elevated thermal readings.

Model	Warning msg.	Warning msg. & Forced Shutdown	
4600T	**53˚C**	**56˚C**	
4600U/T	**CPU 93˚C**	**CPU 98˚C**	
12600U	**43˚C**	**46˚C**	
12620U	**CPU 95˚C**	**CPU 99˚C**	

11.2. Status > Opened Files

This window shows the files in shares that are currently being accessed.



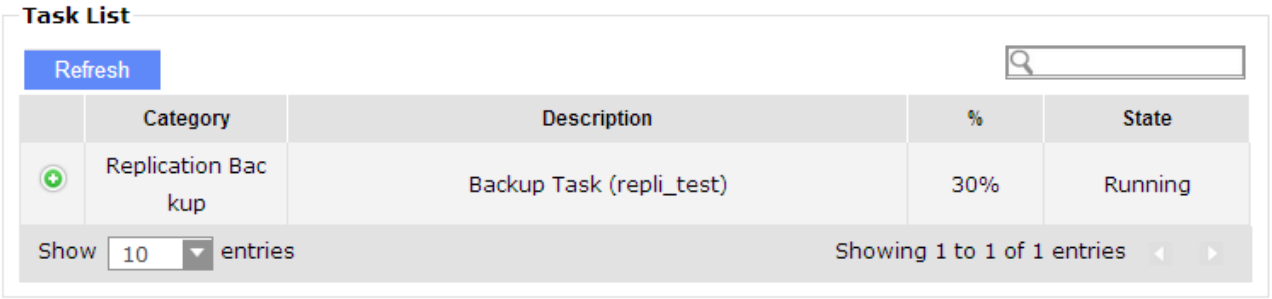
11.3. Status > Connections

This window shows the computers which are currently accessing the shares via SMB, AFP, FTP, HTTP, or iSCSI protocol.

You can use the protocol type, such as keying AFP, to search for the computers that are currently having an access with the NAS server.

11.4. Status > Task Progress

This window shows the tasks currently taking place on your server. For example, the volume sync/Rsync, replication, volume scanning, or the account permission settings with a Windows AD server will be displayed in here.



11.5. Status > Loading

This window shows the visualized display for the consumption of system resources. The loading status include Memory Usage, CPU Summary, Network Summary, and Disk Summary.

For the 12600 series, warning messages will be sent when the system operaing temperature reaches 43º. When the 46ºC threshold is reached, a warning message is delivered and the system will automatically shut down.

When the CPU temperature reaches 95ºC, a warning message will be delivered; and when the 99ºC threshold is reached, a warning message will be delivered and the system will automatically shut down.

Appendix A More about RAID Storage

1. Volume Expansion:

In addition to volumes made of striping, mirroring, RAID-Z1/Z2, several volumes can be combined into a larger volume pool. The combinations can be:

1-1. Mirror + Mirror +...: similar to traditional RAID10.

1-2. RAID-Z1 + RAID-Z1 + ...: similar to RAID50.

1-3. RAID-Z2 + RAID-Z2 +...: similar to RAID60.

2. Volume Characteristics:

The characteristics of different logical volumes can be summarized as follows:

Volume type	Min. no. of disks	Usable capacity	Description
Stripe	1	1	One volume can consist of only a single disk
Mirror	2 or more	1/N	More than 1 disk can fail in a mirrored volume. The max. number of disk failures in a mirrored volume is (N-1).
RAID-Z1	>=3	(N-1)/N	The max. number of disk failure without data loss is 1.
RAID-Z2	>=4	(N-2)/N	The max. number of disk failure without data loss is 2.

3. Volume Online Expansion

3-1. Online Expansion:

If there is any unpopulated disk tray, you can replace any of the disk member in a logical volume. To do that, you can:

3-1-1. Insert a larger new drive in an unused disk bay. Replace an existing member drive using with the new, larger drive.

3-1-2. The process can take hours depending on the size of the volume and the size of the data stored on the volume.

4. Disk Roaming from 4600U/T to 12600U rack-mount models:

4-1. Power down the 4600U/T system.
4-2. Remove all member drives belonging to a logical volume. Re-install them to the drive trays of the 12600U series systems.
4-3. Install these member drives to the 12600U system.
4-4. If the 12600U system is online and running, move to the Storage > Volume page to bring the volume online.
4-5. If the 12600U system is offline, power it on and the volume is automatically brought online later.

5. Faulty disk replacement Procedure:

5-1. If a disk drive fails in an online volume, replace it with a new disk drive. The system will begin the online rebuild.

5-2. If a disk drive fails in an online volume, you can install the replacement drive in an unused disk bay. You can then enter the volume management window and replace the faulty drive with the new, replacement drive.

5-3. If multiple members of a volume have been removed, the system will automatically bring the volume offline.

5-4. An offline volume, (meaning that when a system is powered down; or the members of a volume moved to a different chassis), can have its member drives installed in disorderly drive bay positions. The system will automatically detect the logical volume information and the whereabouts of its members. The user can then bring the volume online.